



V Series

Handheld Terminal



User Manual



Copyright

Copyright © 1996, 1997, 1999, 2001 Best Lock Corporation. All rights reserved. Printed in the United States of America.

Information in this document is subject to change without notice and does not represent a commitment on the part of Best Lock Corporation.

This publication is intended to be an accurate description and set of instructions pertaining to its subject matter. However, as with any publication of this complexity, errors or omissions are possible. Please call your BEST distributor or Best Access Systems at (317) 849-2250 if you see any errors or have any questions. No part of this manual and/or databases may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, without the express written permission of Best Lock Corporation.

This document is distributed as is, without warranty of any kind, either express or implied, respecting the contents of this book, including but not limited to implied warranties for the publication's quality, performance, merchantability, or fitness for any particular purpose. Neither Best Lock Corporation, nor its dealers or distributors shall be liable to the user or any other person or entity with respect to any liability, loss, or damage caused or alleged to be caused directly or indirectly by this publication.

The Best logo is a registered trademark of Best Lock Corporation.

Written and designed by Best Access Systems and Avalon Group, Inc., Indianapolis, Indiana.

T61931 Rev. B 1754626 ER-7991-5

Telephone technical support

Before you call for technical support, please make sure you are at the location where the problem exists, and that you are prepared to provide the following information:

- the exact wording of any error or warning messages
- what you were doing when you encountered the problem and exactly what happened
- what you have done so far to correct the problem.

Best Access Systems representatives provide telephone technical support for all V Series products. You can locate the representative nearest you by calling (317) 849-2250, Monday through Friday, between 7:00 a.m. and 4:00 p.m. eastern standard time; or visit the web page, www.BestAccess.com.

CONTENTS

FIGURES IX

GETTING STARTED 1-1

- Components of the V Series System 1-1
 - Magnetic stripe electronic lock 1-1
 - Proximity reader electronic lock 1-1
 - Keypad electronic lock 1-2
 - Controller 1-2
 - Access cards, card encoder, and Card Encoding Software 1-3
 - Enrolling Station 1-3
 - Programming methods 1-3
 - Handheld terminal 1-3
 - System overview 1-4
- Conventions used in this manual 1-6

HOW DO I PROGRAM A V SERIES SECURITY DEVICE? 2-1

- Overview of programming tasks 2-1
- Tasks to get ready 2-2
- Task 1: Fill out the user forms 2-3
 - Facility Information form 2-3
 - Token & Door Information form and
Token by Door Information form 2-3
- Task 2: Task 2: Encode access cards or generate codes (optional) 2-9
- Task 3: Task 3: Connect the handheld terminal to
the V Series Security Device 2-9
- Tasks to define device settings 2-11
- Task 4: Task 4: Set the date and time 2-12
- Task 5: Task 5: Add holidays 2-13

Task 6: Task 6: Define time zones	2-14
What is a time zone?	2-14
What is a time interval?	2-15
Defining time zone numbers	2-15
How do I define time zones and their intervals?	2-15
Task 7: Task 7: Change the token format (optional)	2-18
Defining the facility code format	2-19
Defining the card number/access code format	2-19
Defining the issue code format	2-19
Using the look ahead feature	2-19
Defining the token length	2-20
Determining whether to validate the LRC	2-20
Task 8: Task 8: Add facility codes	2-27
What is a facility code?	2-27
Task 9: Task 9: Define V Series Controller features (controller only)	2-29
Using the RQE unlock feature	2-30
Using the remote unlock feature	2-30
Selecting the door contact type	2-30
Defining the door open too long feature	2-30
Selecting the door forced alarm feature	2-31
Selecting the alarm output duration	2-31
Task 10: Task 10: Set the chassis type (electronic lock only)	2-35
Task 11: Task 11: Program timed access features	2-36
Setting the unlock duration	2-36
Selecting the door lock time zone	2-37
Selecting the facility code only time zone	2-38
Selecting the door unlock time zone	2-39
Tasks to define the user database	2-41
Task 12: Task 12: Add a communication token and password	2-41
Task 13: Task 13: Add tokens	2-43
Assigning the time zone	2-43
Setting deadbolt override	2-43
Setting passage mode	2-43
Task 14: Task 14: Delete the temporary operator token	2-46
Task 15: Task 15: Add a range of access cards (optional—magnetic stripe security device or proximity security device only)	2-46
Task 16: Task 16: Verify the user database	2-48
Final task	2-50
Task 17: Task 17: Disconnect the handheld terminal	2-50
Programming other V Series Security Devices	2-50

HOW DO I MAINTAIN THE V SERIES SYSTEM? 3-1

Changing a V Series Security Device's user database 3-2

Adding tokens 3-2

Modifying tokens 3-2

Deleting tokens 3-4

Adding a range of access cards 3-5

Deleting a range of access cards 3-5

Programming a V Series Security Device to override time zone control 3-6

Viewing a V Series Security Device's history 3-9

Viewing a V Series Security Device's system data 3-10

Resetting a V Series Security Device 3-10

Clearing a low battery message (electronic lock only) 3-12

GLOSSARY A-1

FIGURES

GETTING STARTED

[V Series System Components](#) 1-5

HOW DO I PROGRAM A V SERIES SECURITY DEVICE?

[Sample of a completed Token & Door Information form](#) 2-5

[Sample of a completed Facility Information form \(front\)](#) 2-6

[Sample of a completed Facility Information form \(back\)](#) 2-7

[Sample of a completed Token by Door Information form](#) 2-8

[Connecting the handheld to the device](#) 2-11

[Defining time zones and their intervals—an example](#) 2-16

1

GETTING STARTED

This manual describes how to use a V Series Handheld Terminal to program and maintain electronic locks and controllers in a V Series System. Each V Series Security Device provides a variety of programmable features that determine how the device operates and when users gain access to the door controlled by the device.

The handheld is a passive programming device, which relies on the V Series Security Device's firmware to run. When connected to a device, the handheld lets you define or change the device's programming settings and user database. Also, the handheld lets you view a history of up to 1000 events at the device.

COMPONENTS OF THE V SERIES SYSTEM

Magnetic stripe electronic lock

One of the main components of the V Series System is the magnetic stripe electronic lock. This lock can be accessed by inserting and removing a valid magnetic stripe card in the lock. The lock can be programmed using a PC running SMART or the IPS for Windows, or a V Series Handheld Terminal.

Proximity reader electronic lock

Another main component of the V Series System is the proximity electronic lock. This lock, which is well-suited for outdoor locations, can be accessed by holding a valid proximity card near the lock. It supports HID and Motorola/Indala proximity cards,

and is compatible with Weigand, ABA, and custom-formatted proximity cards. The lock can be programmed using a PC running the IPS or the IPS for Windows, or a handheld.

Keypad electronic lock

Another main component of the V Series System is the keypad electronic lock. This lock can be accessed by entering a personal identification number (PIN) on the lock's keypad. This lock, which is well-suited for outdoor locations, serves as an alternative to the magnetic stripe electronic lock and the proximity electronic lock. The user does not have to carry a card to access the keypad electronic lock.

The keypad electronic lock can be programmed using a PC running the IPS or the IPS for Windows, or a handheld. Also, some programming can be performed directly from the lock's keypad.

Controller

The V Series Controller allows the V Series electronics to be separate from the door's locking mechanism and to be located up to 500 feet away from the locking mechanism. The controller provides V Series electronic features for use with electrically-controlled locking devices.

The controller is well-suited to provide access control for:

- exit devices
- glass doors
- non-standard doors
- turnstiles
- doors controlled by electric strikes or magnetic locks
- electrically-operated mortise or cylindrical locks.

The controller is suitable for use with interior or exterior doors. The controller has an adaptable power supply input that accepts 12 or 24 volts AC or DC. A backup battery supports the controller's programming in the event of a power failure. All controller functions are shut down while under backup power.

The main role of the controller is to control the operation of the locking device connected to the controller. A reader can be connected to the controller to provide a means for users to access the door controlled by the controller.

The controller can accept a request-to-exit signal from a lock, or a separate request-to-exit device, such as a button, that is connected to the controller. When someone turns a door knob with a request-to-exit feature, or presses a request-to-exit button, the controller does not trigger an alarm when the door is opened. If the controller is programmed for the RQE unlock feature, the controller also unlocks the door.

A remote unlock device, such as a button, can be connected to a controller. This device can be located away from the door. When

someone, such as a receptionist, presses the remote unlock button, the controller unlocks the door if the controller is programmed for the remote unlock feature.

The controller can monitor the door's status. If the door is opened without use of a valid access method, the controller can trigger a door forced alarm. The controller can monitor whether the door has been open too long. The controller also can supervise a tamper switch, which can be used to protect the controller enclosure or another device. The controller's alarm output can trigger an external alerting device, such as a siren or strobe light, or a security system.

Access cards, card encoder, and Card Encoding Software

The magnetic stripe electronic lock accepts magnetic stripe cards produced by a variety of manufacturers, as well as magnetic stripe cards manufactured by BEST. If your system uses magnetic stripe cards manufactured by BEST, you can obtain encoded cards from your BEST representative, or you can encode your system's access cards yourself.

To encode access cards, you need:

- an IBM-compatible PC with a 386 or higher speed processor, 4 MB of RAM (random access memory), at least 10 MB of free hard disk space, Microsoft Windows 3.1
- a V Series Card Encoder, obtained from BEST
- the V Series Card Encoding Software, obtained from BEST.

Enrolling Station

The VPD-ES Enrolling Station can be connected to a PC running the IPS and used to read proximity cards while adding token records to a device configuration used by proximity security devices. The enrolling station works with a variety of common proximity card formats. For a list of compatible card formats, refer to the *VPD-ES Enrolling Station Setup and Operating Instructions*.

Programming methods

Each V Series Security Device provides a variety of programmable features that determine how the device operates and when users gain access to the door. The device can be programmed using either a V Series Handheld Terminal, or a palmtop PC or laptop PC running the V Series Intelligent Programmer Software (IPS). Additionally, limited programming can be performed for a V Series Keypad Security Device using its keypad.

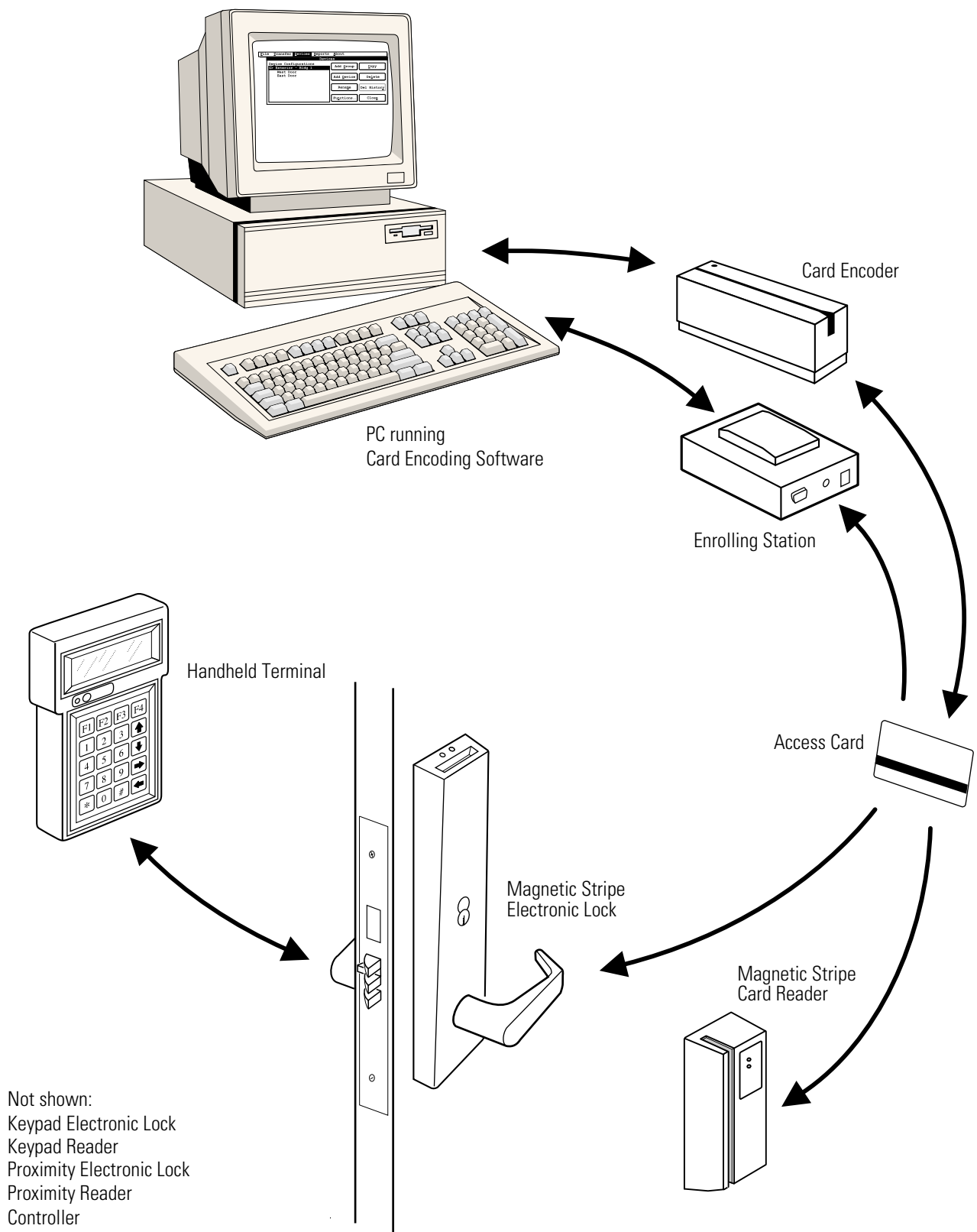
Handheld terminal

The V Series Handheld Terminal is a passive programming device, which relies on the V Series Security Device's firmware to run. The handheld lets you define or change a device's programming settings and user database only when the handheld is connected to the device. When connected to the device, the handheld also lets you view a history of up to 1000 events at the device. The handheld does not store any information.

**System
overview**

Figure 1.1 shows the main components of a V Series System that uses a handheld to program and maintain devices. The table below defines each of the possible components in the V Series System. Keep in mind that your system might not include all of these components.


Component	Definition
Card encoder	Device that reads, encodes, and erases information on a magnetic stripe card.
Card Encoding Software	Software that controls the card encoder.
Controller	Device that allows the V Series electronics to be separate from a door's locking mechanism and to be located up to 500 feet away from the locking mechanism. The controller provides V Series electronic features for use with electrically-controlled locking devices. A reader can be connected to the controller to provide a means for users to access the door.
Electronic lock	A battery-powered, self-contained, programmable lock that controls access to a door.
Enrolling Station	Device that can be connected to a PC running IPS and used to read proximity cards while adding token records to a device configuration used by proximity security devices.
Handheld terminal	Device that lets you define programming settings and the user database for a V Series Security Device—an electronic lock or controller. It also lets you view access control information, such as the user database, configuration settings, and event history. The handheld is the only equipment necessary to program and maintain the device.
Intelligent Programmer Software (IPS) or Intelligent Programmer Software (IPS) for Windows	Software that lets you define programming settings and the user database for groups of V Series Security Devices, as well as individual devices. You also can use the IPS to retrieve the history records from devices. The IPS lets you view and print information about devices at any time.
Token	An access card or personal identification number (PIN) containing identification information. A token is given to a user and is similar to a key, letting the user gain access to a controlled area.

**Figure 1.1** V Series System Components

CONVENTIONS USED IN THIS MANUAL

Each activity described in this manual begins with a brief explanation of its purpose. To help you select programming settings, read this explanation before you perform the activity.

Step-by-step instructions also are provided for each activity. To help you understand the steps provided for activities, review the table below, which describes the conventions used in this manual.

Convention	Explanation
Information introduced by Note:	Information that clarifies a discussion or additional information that might be of interest.
Information introduced by Tip:	Information that indicates a helpful hint for performing a step or activity.
 Caution	Icon indicating a warning about the possible consequences of actions that might cause equipment to be damaged or information to be lost.
BOLD	Information you type or would type if you were entering the information provided in an example.
Numbered steps introduced by a phrase such as, To add a token:	Step-by-step procedure for performing an activity.
The word device	Short-hand way of referring to either: <ul style="list-style-type: none">■ a V Series Magnetic Stripe Security Device (a magnetic stripe electronic lock or controller)■ a V Series Proximity Security Device (a proximity electronic lock or controller)■ a V Series Keypad Security Device (a keypad electronic lock or controller).
The word token	Short-hand way of referring to either: <ul style="list-style-type: none">■ a card that a user uses to access a door with a V Series Magnetic Stripe Security Device■ a card that a user uses to access a door with a V Series Proximity Security Device■ a personal identification number (PIN) that a user enters to access a door with a V Series Keypad Security Device.

2

HOW DO I PROGRAM A V SERIES SECURITY DEVICE?

OVERVIEW OF PROGRAMMING TASKS

To program a V Series Security Device, you need to gather information about how you want the device to work. Then you connect the V Series Handheld Terminal to the device and program the device. Use the checklist on the next page, which shows each group of tasks you need to perform, to make sure you perform each task.

Tasks to get ready

- ☐ Task 1: Fill out the user forms. See [page 2-3](#).
- ☐ Task 2: Encode access cards or generate codes (optional). See [page 2-9](#).
- ☐ Task 3: Connect the handheld terminal to the V Series Security Device. See [page 2-9](#).

Tasks to define device settings

- ☐ Task 4: Set the date and time. See [page 2-12](#).
- ☐ Task 5: Add holidays. See [page 2-13](#).
- ☐ Task 6: Define time zones. See [page 2-14](#).
- ☐ Task 7: Change the token format (optional). See [page 2-18](#).
- ☐ Task 8: Add facility codes. See [page 2-27](#).
- ☐ Task 9: Define V Series Controller features (controller only). See [page 2-29](#).
- ☐ Task 10: Set the chassis type (electronic lock only). See [page 2-35](#).
- ☐ Task 11: Program timed access features. See [page 2-36](#).

Tasks to define the user database

- ☐ Task 12: Add a communication token and password. See [page 2-41](#).
- ☐ Task 13: Add tokens. See [page 2-43](#).
- ☐ Task 14: Delete the temporary operator token. See [page 2-46](#).
- ☐ Task 15: Add a range of access cards (optional—magnetic stripe security device or proximity security device only). See [page 2-46](#).
- ☐ Task 16: Verify the user database. See [page 2-48](#).

Final task

- ☐ Task 17: Disconnect the handheld terminal. See [page 2-50](#).

TASKS TO GET READY

This section describes the following tasks, which you perform before you begin to program the device:

- Task 1: Fill out the user forms. See [page 2-3](#).
- Task 2: Encode access cards or generate codes (optional). See [page 2-9](#).
- Task 3: Connect the handheld terminal to the V Series Security Device. See [page 2-9](#).

TASK 1: FILL OUT THE USER FORMS

Use the Facility Information form, the Token & Door Information form, and the Token by Door Information form to collect the information needed to program the V Series Security Devices in your facility. You'll use the information to determine how each device operates and how users gain access to each device.

You'll find it easier to fill out the user forms if you first read this entire chapter. The section *Task 6: Define time zones* on [page 2-14](#) is especially helpful.

Facility Information form

Use the Facility Information form to collect information about your facility and its operation. [Figure 2.2](#) and [Figure 2.3](#) show a sample of a completed form.

Follow the instructions on the form to provide the information necessary for your facility. Leave blank any sections that don't apply.

Token & Door Information form and Token by Door Information form

The Token & Door Information form and the Token by Door Information form help you determine

- the information necessary to configure the device for each door
- the user data necessary to provide people access to each door.


Follow the instructions on the selected form to provide the information necessary for each door in your facility. Leave blank any sections that don't apply.

Use either the Token & Door Information form or the Token by Door Information form. You don't need to complete both forms. The Token & Door Information form is best suited to smaller facilities. The Token by Door Information form is best suited to larger facilities.

[Figure 2.1](#) shows a sample of the first page of a completed Token & Door Information form. [Figure 2.4](#) shows a sample of the first page of a completed Token by Door Information form.

Record information common to all doors

Record information common to all tokens



V Series System Token & Door Information

Instructions: Tokens are either access cards or personal identification numbers (PINs). Group users with like access together. List card numbers/access codes in numerical order. If some or all access information is common to all tokens, use **Note A** to the right.

Card Nos / Codes	IC No. Name	ALL DOORS	Door Front	Door Back	Door Suite	Door	Door	Door
		UD sec.	UD 10 sec.	UD 10 sec.	UD 10 sec.	UD sec.	UD sec.	UD sec.
SN 500003 CN	1 John Boss	DL TZ FC TZ DU TZ 1st Crd Unlck Controller	DL TZ FC TZ DU TZ 1st Crd Unlck Controller	DL TZ FC TZ DU TZ 1st Crd Unlck Controller	DL TZ FC TZ DU TZ 1st Crd Unlck Controller	DL TZ FC TZ DU TZ 1st Crd Unlck Controller	DL TZ FC TZ DU TZ 1st Crd Unlck Controller	DL TZ FC TZ DU TZ 1st Crd Unlck Controller
SN 500004 CN	2 Jacques Elul	DL TZ FC TZ DU TZ 1st Crd Unlck Controller	DL TZ FC TZ DU TZ 1st Crd Unlck Controller	DL TZ FC TZ DU TZ 1st Crd Unlck Controller	DL TZ FC TZ DU TZ 1st Crd Unlck Controller	DL TZ FC TZ DU TZ 1st Crd Unlck Controller	DL TZ FC TZ DU TZ 1st Crd Unlck Controller	DL TZ FC TZ DU TZ 1st Crd Unlck Controller
SN 500005 CN	1 James Herin	DL TZ FC TZ DU TZ 1st Crd Unlck Controller	DL TZ FC TZ DU TZ 1st Crd Unlck Controller	DL TZ FC TZ DU TZ 1st Crd Unlck Controller	DL TZ FC TZ DU TZ 1st Crd Unlck Controller	DL TZ FC TZ DU TZ 1st Crd Unlck Controller	DL TZ FC TZ DU TZ 1st Crd Unlck Controller	DL TZ FC TZ DU TZ 1st Crd Unlck Controller
SN 500006 CN	1 Jacqueline Murawski	DL TZ FC TZ DU TZ 1st Crd Unlck Controller	DL TZ FC TZ DU TZ 1st Crd Unlck Controller	DL TZ FC TZ DU TZ 1st Crd Unlck Controller	DL TZ FC TZ DU TZ 1st Crd Unlck Controller	DL TZ FC TZ DU TZ 1st Crd Unlck Controller	DL TZ FC TZ DU TZ 1st Crd Unlck Controller	DL TZ FC TZ DU TZ 1st Crd Unlck Controller
SN 500007 CN	1 Nicolas Copernicus	DL TZ FC TZ DU TZ 1st Crd Unlck Controller	DL TZ FC TZ DU TZ 1st Crd Unlck Controller	DL TZ FC TZ DU TZ 1st Crd Unlck Controller	DL TZ FC TZ DU TZ 1st Crd Unlck Controller	DL TZ FC TZ DU TZ 1st Crd Unlck Controller	DL TZ FC TZ DU TZ 1st Crd Unlck Controller	DL TZ FC TZ DU TZ 1st Crd Unlck Controller
SN 500008 CN	1 Martin Van Buren	DL TZ FC TZ DU TZ 1st Crd Unlck Controller	DL TZ FC TZ DU TZ 1st Crd Unlck Controller	DL TZ FC TZ DU TZ 1st Crd Unlck Controller	DL TZ FC TZ DU TZ 1st Crd Unlck Controller	DL TZ FC TZ DU TZ 1st Crd Unlck Controller	DL TZ FC TZ DU TZ 1st Crd Unlck Controller	DL TZ FC TZ DU TZ 1st Crd Unlck Controller

Note A: Information common to all tokens
 TZ for all tokens
 DBO for all tokens
 PM for all tokens
 Expiration date for all tokens 01/12/31

Note B: Abbreviations
 AD = DONTL alarm duration
 AOD = Alarm output duration
 CN = Card no./access code
 DBO = Deadbolt override
 DD = DONTL delay duration
 DL TZ = Door lock time zone
 DONTL = Door open too long
 DU TZ = Door unlock time zone
 FC TZ = Facility code only time zone
 IC = Issue code
 PM = Passage mode
 S/N = Serial number
 UD = Unlock duration
 WD = DONTL warning duration

Reference the abbreviations

E-771A 3/97

Facility Administration Building Department /Division _____

Approval John A. Boss Date 12/1/00 Page 1 of 8

Figure 2.1 Sample of a completed Token & Door Information form

Define up to
16 holidays



V Series System Facility Information

Holidays

Holidays are time periods usually associated with calendar holidays. Each holiday can span any time period you designate. For example, a holiday might be defined as half a day. Another holiday might span an entire week. For each holiday, you provide the date and time when the holiday starts, as well as the date and time when the holiday ends. For a 24-hour holiday, list the start time as 00:00 and the end time as 23:59. **Caution: Make sure that you schedule to reprogram holidays after the last holiday expires. Failure to reprogram holidays will allow users access on those days that would otherwise have been programmed as holidays.**

	Holiday	Start		End	
		Yr./Mo./Day	Time	Yr./Mo./Day	Time
1	MLK Jr.'s Birthday	00/01/15	00:00	00/01/15	23:59
2	President's Day	00/01/19	00:00	00/01/19	23:59
3	Spring Holiday	00/04/04	18:00	00/04/08	06:00
4	Memorial Day Weekend	00/05/25	00:00	00/05/28	06:00
5	Independence Day Weekend	00/07/04	00:00	00/07/08	06:00
6	Labor Day Weekend	00/08/31	00:00	00/09/03	06:00
7	Fall Holiday	00/10/10	18:00	00/10/15	06:00
8	Thanksgiving Holiday	00/11/27	16:00	00/12/02	06:00
9	Christmas Holiday	00/12/23	18:00	00/12/27	06:00
10		/ /	:	/ /	:
11		/ /	:	/ /	:
12		/ /	:	/ /	:
13		/ /	:	/ /	:
14		/ /	:	/ /	:
15		/ /	:	/ /	:
16		/ /	:	/ /	:

Define up to
8 time zones

Time zones

Time zones are regular blocks of time that schedule when users have access, and when doors automatically change modes. Each time zone may have one, two, or three time intervals. Time intervals are a way to add flexibility to the time zone. For example, time zone 1 could be divided into two time intervals, such as 8:00–12:00 and 13:00–17:00 (24-hour time). The time zone would be inactive from 12:00–13:00.

Use 24-hour time to define time intervals. "H" stands for holiday. "D" stands for Sunday. Define up to eight time zones below. Then, assign the time zones on the *V Series System Token & Door Information* or the *V Series System Token by Door Information* form.

TZ 1		Start time	Stop time	D	M	T	W	T	F	S	H	TZ 5		Start time	Stop time	D	M	T	W	T	F	S	H
TI 1		00:00	23:59	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	TI 1		09:30	11:30	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
TI 2		00:00	06:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	TI 2				<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
TI 3		12:00	23:59	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	TI 3				<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
TZ 2		Start time	Stop time	D	M	T	W	T	F	S	H	TZ 6		Start time	Stop time	D	M	T	W	T	F	S	H
TI 1		07:00	18:00	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	TI 1		09:00	10:00	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
TI 2				<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	TI 2				<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
TI 3				<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	TI 3				<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
TZ 3		Start time	Stop time	D	M	T	W	T	F	S	H	TZ 7		Start time	Stop time	D	M	T	W	T	F	S	H
TI 1		07:00	13:00	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	TI 1				<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
TI 2		11:30	17:30	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	TI 2				<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
TI 3				<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	TI 3				<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
TZ 4		Start time	Stop time	D	M	T	W	T	F	S	H	TZ 8		Start time	Stop time	D	M	T	W	T	F	S	H
TI 1		17:00	23:59	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	TI 1				<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
TI 2				<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	TI 2				<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
TI 3				<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	TI 3				<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

E-770A 3/97

Figure 2.2 Sample of a completed Facility Information form (front)

Record facility code information

Facility codes

Facility codes assigned by your BEST representative are unique codes that must be programmed into every V Series Security Device and encoded on every access card, or included in every personal identification number (PIN). The facility code ensures the facility's security since an access card or PIN without the facility code cannot gain access. You can enter a maximum of eight unique facility codes in each device. In most cases only one facility code will ever be used.

PINs are managed using one number—the access code, which uniquely identifies each user. Use the "Card no./Code" column to record this number.

You can manage access cards with one or two numbers. In most cases, the card serial number—the number printed on the back of every access card—is the number that is encoded on the card. This six-digit number is used both for physical identification and as the number that is programmed into the device. But for added security, the card number encoded on the access card can be different than the card serial number. If this is the case, use the "Card/Code no." column. Otherwise, leave it blank.

	Facility code	Starting card nos./access codes		Ending card nos./access codes	
		Card serial no.	Card no./Code	Card serial no.	Card no./Code
1	13579	500001		500599	
2					
3					
4					
5					
6					
7					
8					

Record the communication token information

Configure system—Communication tokens

The communication token lets you communicate with the V Series Security Device and configure the system. The temporary communication token, provided with every device, is for temporary use only, and only lets you communicate with a factory default device.

Caution: Be sure to delete the temporary communication token and add the permanent communication token(s). Failure to replace the temporary communication token can lock you out of all programming functions.

	Card serial no.	Card no./Code
Communication token #1	500001	
Communication token #2		

Check to enable daylight savings time

Daylight savings time

The time in the V Series Security device can be programmed to automatically adjust when daylight savings time starts and ends. Check the box if your locality observes daylight savings time. Daylight savings time in the United States starts at 2:00 A.M. on the first Sunday in April, and ends at 2:00 A.M. on the last Sunday in October.

☒ Enable daylight savings time

Notes & comments

Use the same holidays for all the doors in the building.

Facility Administration Building Location Corporate Office
 Approval John A. Boss Title Bldg. Mngr. Date 12/1/00


E-770B 3/97

Figure 2.3 Sample of a completed Facility Information form (back)

Record the doors this information is for

Record information common to the doors

Record information for each token



V Series System

Token by Door Information

Door Information

This information is for:

☐ All doors

☐ One door _____

☒ A group of doors (example: exterior doors)
Main exterior doors

Unlock duration 10 sec.

Door Lock TZ 0

Facility Code TZ 6

Door Unlock TZ 5

☒ First card unlock

☐ Controller

Door contact: ☐ NC ☐ NO

☐ Door Forced alarm

☐ RQE Unlock

☐ Remote Unlock

☐ Door Open Too Long alarm

Delay duration _____ sec.

Warning duration _____ sec.

Alarm duration _____ sec.

Alarm output duration _____ sec.

Token Information

Tokens are either access cards or personal identification numbers (PINs). Group users with like access together. List card numbers or access codes in numerical order.

Information common to all tokens:

Time zone for all tokens _____

☒ Deadbolt override (mortise locks only)

☐ Passage mode

Expiration date 01 / 12 / 31

Card No./Code	Issue Code	Name	Access Information
Serial No. <u>500003</u> Card No./Code	<u>1</u>	<u>John Boss</u>	Time zone <u>1</u> <input checked="" type="checkbox"/> Deadbolt override <input checked="" type="checkbox"/> Passage mode Expires: ____/____/____
Serial No. <u>500004</u> Card No./Code	<u>1</u>	<u>John Smith</u>	Time zone <u>1</u> <input checked="" type="checkbox"/> Deadbolt override <input checked="" type="checkbox"/> Passage mode Expires: ____/____/____
Serial No. <u>500005</u> Card No./Code	<u>2</u>	<u>Jacques Ellul</u>	Time zone <u>2</u> <input checked="" type="checkbox"/> Deadbolt override <input type="checkbox"/> Passage mode Expires: ____/____/____
Serial No. <u>500006</u> Card No./Code	<u>1</u>	<u>Margaret Keller</u>	Time zone <u>1</u> <input checked="" type="checkbox"/> Deadbolt override <input checked="" type="checkbox"/> Passage mode Expires: ____/____/____
Serial No. <u>500007</u> Card No./Code	<u>1</u>	<u>James Herin</u>	Time zone <u>2</u> <input checked="" type="checkbox"/> Deadbolt override <input type="checkbox"/> Passage mode Expires: ____/____/____
Serial No. <u>500008</u> Card No./Code	<u>1</u>	<u>Jacqueline Murawski</u>	Time zone <u>2</u> <input checked="" type="checkbox"/> Deadbolt override <input type="checkbox"/> Passage mode Expires: ____/____/____
Serial No. <u>500009</u> Card No./Code	<u>1</u>	<u>Nicolas Copernicus</u>	Time zone <u>3</u> <input checked="" type="checkbox"/> Deadbolt override <input type="checkbox"/> Passage mode Expires: ____/____/____
Serial No. <u>500010</u> Card No./Code	<u>1</u>	<u>Martin Van Buren</u>	Time zone <u>9</u> <input checked="" type="checkbox"/> Deadbolt override <input type="checkbox"/> Passage mode Expires: ____/____/____
Serial No. <u>500011</u> Card No./Code	<u>1</u>	<u>William Blake</u>	Time zone <u>2</u> <input checked="" type="checkbox"/> Deadbolt override <input type="checkbox"/> Passage mode Expires: ____/____/____
Serial No. <u>500012</u> Card No./Code	<u>1</u>	<u>David Crockett</u>	Time zone <u>3</u> <input checked="" type="checkbox"/> Deadbolt override <input type="checkbox"/> Passage mode Expires: ____/____/____
Serial No. <u>5000013</u> Card No./Code	<u>1</u>	<u>Jane Jones</u>	Time zone <u>3</u> <input checked="" type="checkbox"/> Deadbolt override <input type="checkbox"/> Passage mode Expires: ____/____/____

Facility Administration Building

Department /Division _____

Approval John A Boss

Date 12/1/00

E-775A 3/97

Page 1

Figure 2.4 Sample of a completed Token by Door Information form

TASK 2: ENCODE ACCESS CARDS OR GENERATE CODES (OPTIONAL)

Next, you can encode the access cards or generate the access codes for people who will have access to your facility. For instructions on using the V Series Card Encoding Software, use the software's on-line help feature. If you don't have a card encoder, your cards are pre-programmed for you. If you want BEST to generate random access codes for you, contact your BEST representative.

TASK 3: CONNECT THE HANDHELD TERMINAL TO THE V SERIES SECURITY DEVICE

You enable communication between the handheld terminal and the V Series Security Device by connecting one end of a handheld-to-device cable to the handheld and the other end to the device, and by using the temporary communication token to access the device. The handheld-to-device cable is provided with the handheld. The temporary communication token is provided with the device.

Before you connect the handheld to the device, make sure you understand the terms and definitions described in the table below.

Term	Definition
Handheld terminal	Device that lets you define programming settings and the user database for a V Series Security Device—an electronic lock or controller. It also lets you view access control information, such as the user database, configuration settings, and event history. The handheld is the only equipment necessary to program and maintain the device.
Temporary communication token	Access card or personal identification number (PIN) for temporary use that lets you communicate with a V Series Security Device programmed with factory default settings.
Temporary operator token	Access card or PIN that gives people temporary access before the devices in the V Series system are permanently programmed. For example, workers can use this token to access the facility while it is under construction, but they will not have access when construction is finished.



If you disconnect the handheld without programming a facility code and a permanent communication token, you won't be able access the device. If you can't get back into a device, see the V Series Service Manual, Emergency Operations section. When programming the device, the device exits communication mode after 5 minutes of inactivity. To reactivate it, use the communication token. (If you're programming a V Series Controller, place DIP switch 6 on the controller board in the ON position before you use the communication token.)

To connect the handheld to the device:

1. Refer to [Figure 2.5](#) and plug the handheld-to-device cable into the base of the electronic lock or the handheld connector on the controller.
2. If you're programming a controller, place DIP switch 6 on the controller board in the ON position.
3. Plug the handheld-to-device cable into the base of the handheld.
4. Press the handheld's **ON/OFF** button.
5. Use the temporary communication token to access the device.

Note: If PINs have five digits by default, the temporary communication PIN is 99999. If PINs have twelve digits by default, the temporary communication PIN is 999999999990 (eleven 9s, and one 0).

You see:

PASSWORD: *****

6. Type **123456** (the default password).
7. Press *. You see:

>ENTER DATE/TIME
CONFIG HOLIDAYS

Note: To disconnect the handheld when you've finished programming the device, see [page 2-50](#).

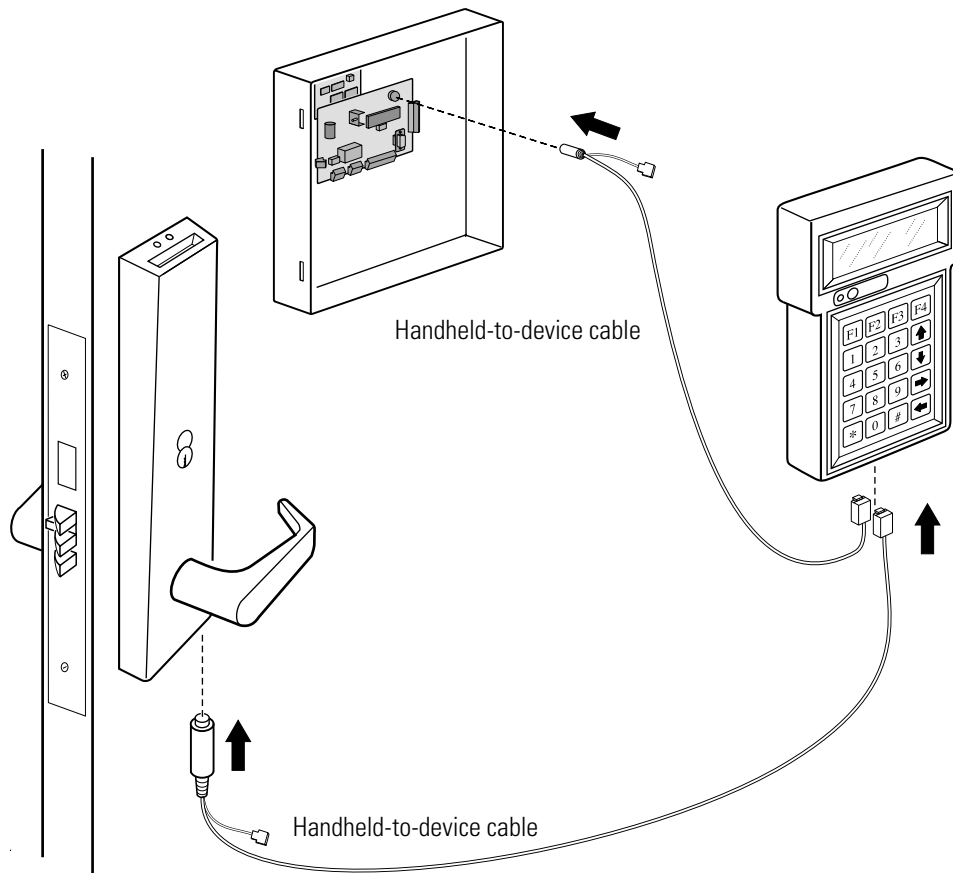


Figure 2.5 Connecting the handheld to the device

TASKS TO DEFINE DEVICE SETTINGS

This section describes the following tasks, which you perform to define settings that determine the operation of the V Series Security Device:

- Task 4: Set the date and time. See [page 2-12](#).
- Task 5: Add holidays. See [page 2-13](#).
- Task 6: Define time zones. See [page 2-14](#).
- Task 7: Change the token format (optional). See [page 2-18](#).
- Task 8: Add facility codes. See [page 2-27](#).
- Task 9: Define V Series Controller features (controller only). See [page 2-29](#).
- Task 10: Set the chassis type (electronic lock only). See [page 2-35](#).
- Task 11: Program timed access features. See [page 2-36](#).

TASK 4: SET THE DATE AND TIME

Each V Series Security Device has an internal clock/calendar that keeps track of the current date and time. The device needs to know the date and time to operate correctly and to keep an accurate record of all events at the device.

When you first program the device, you need to set the correct date and time. You also need to indicate whether the device is located in an area that changes to daylight savings time for part of the year. If you program the device for daylight savings time, the device automatically adjusts its clock ahead one hour in the spring and back one hour in the fall on the appropriate dates.

Note: In the U.S., daylight savings time begins on the first Sunday in April at 2:00 a.m. and ends on the last Sunday in October at 2:00 a.m.

To set the date and time:

1. Press ↑ or ↓ until you see:

>ENTER DATE/TIME
CONFIG HOLIDAYS

2. Press *. For example, you see:

YY/MM/DD
DATE 92/01/01

3. Type today's date, first typing the year, then the month, then the day.

For example, to enter December 1, 2000, type **001201**.

4. Press *.

The handheld automatically displays the day of the week corresponding to the date you entered. For example, you see:

> SUNDAY
MONDAY

Make sure the selected day is correct. If the day is incorrect, the date is incorrect. Press # and repeat Step 1 through Step 4.

5. Press *. For example, you see:

HH:MM
TIME 12:30

6. Type the current time in 24-hour format.

For example, to enter 5:05 p.m., type **1705**.

7. Press *. You see:

```
DAYLIGHT SAVINGS
0=NO 1=YES: 1
```

8. If the device is located in an area that changes to daylight savings time, type **1**.

If the device is located in an area that does not change to daylight savings time, type **0**.

9. Press *. You see:

```
>ENTER DATE/TIME
CONFIG HOLIDAYS
```

TASK 5: ADD HOLIDAYS

To configure the V Series Security Device for operation on holidays, you need to define each holiday you listed on the Facility Information form when you performed Task 1 (see [page 2-3](#)). A holiday is a time period usually associated with a calendar holiday. You can program up to 16 holidays.

Each holiday can span any time period you designate. For example, one holiday might be defined as half a day. Another holiday might span an entire week. For each holiday, you program the date and time when the holiday starts, as well as the date and time when the holiday ends.

Note: Do not enter 24:00 to indicate the end of a holiday. Instead, enter 23:59.

To add a holiday:

1. Press ↑ or ↓ until you see:

```
>CONFIG HOLIDAYS
ENTER TIME ZONE
```

2. Press *. You see:

```
>HOLIDAY 01
HOLIDAY 02
```

3. Press *. You see:

```
01 YY/MM/DD HH:MM
START 00/00/00-00:00
```

4. Type the date and time when the holiday will start. For the date, type the year, then the month, then the day. For the time, use the 24-hour format.

For example, if the holiday will start on December 31, 2000 at 1:00 p.m., type **0012311300**.

5. Press *. You see:

01 YY/MM/DD HH:MM
END 00/00/00-00:00

6. Type the date and time when the holiday will end.

For example, if the holiday will end on January 2, 2001 at 7:00 a.m., type **0101020700**.

7. Press *. You see:

>HOLIDAY 02
HOLIDAY 03

8. For each additional holiday you want to program, repeat Step 3 through Step 7.
9. When you've added all the holidays you want, press #. You see:

>CONFIG HOLIDAYS
ENTER TIME ZONE

TASK 6: DEFINE TIME ZONES

Before you can program the V Series Security Device with the settings that determine when each valid token can access the door controlled by the device, and with settings that determine when special access features are in effect, you need to define the time zones for the device. Use the information you provided on the Facility Information form in Task 1 (see [page 2-3](#)).

In this task, you define when each time zone occurs. You'll use these time zones when you perform Task 11 to program timed access features and Task 13 to add tokens.

What is a time zone?

Time zones are blocks of time that occur each week and/or on holidays. You define time zones to set up days and times when:

- valid tokens can access the door controlled by the device
- the door automatically unlocks (or unlocks when a valid token accesses the door) and then later relocks
- all tokens in the facility can access the door
- the door automatically locks down, denying *all* tokens access, and then later resumes normal operation.

What is a time interval?

Each time zone can have up to three intervals. Intervals are time periods when selected tokens can access the door or a special access feature is in effect. For each interval, you define the start time and end time. You also indicate which days each interval is in effect.

Each time zone can have up to three intervals. If the time zone spans midnight, you must define two intervals—one before midnight and one after midnight.

Note: Do not enter 24:00 to indicate the start time of a time interval. Instead, enter 00:00.

Defining time zone numbers

You can define the time zones numbered one through eight. However, Time Zone 0 and Time Zone 9 are already defined for you.

- Time Zone 0 = Never
- Time Zone 9 = Always (24 hours per day, 7 days per week, (plus holidays))

How do I define time zones and their intervals?

The best way to understand how to define time zones and intervals is to consider an example. Suppose the device you're programming is on a door that provides access to the offices for an entire department. Also, suppose the door needs to be accessed by the following groups of employees:

- **Managers.** Managers are allowed to access the door any time except on Sunday mornings from 6:00 a.m. until noon and on holidays.
- **Full-time employees.** Full-time employees are allowed to access the door from 7:00 a.m. until 6:00 p.m. on Mondays through Fridays.
- **Several part-time employees.** Part-time employees are allowed to access the door from 7:00 a.m. until 1:00 p.m. on Mondays, Wednesdays, and Fridays. They're also allowed to access the door on Saturdays from 11:30 a.m. until 5:30 p.m.
- **Housekeeping staff.** Housekeeping personnel are allowed to access the door from 5:00 p.m. until midnight on Sundays through Thursdays.
- **Security staff.** Security personnel are allowed to access the door at any time, including on Holidays.

Suppose you also want to enable the following features for the door:

- The door should automatically unlock on Thursdays at 9:30 a.m. and then relock at 11:30 a.m. Each week during this time, participants in a local professional association hold a meeting at the department's offices. Participants include employees from other companies, who don't have tokens for the facility.
- The device should let all tokens in the facility access the door on Mondays from 9:00 a.m. until 10:00 a.m. Each week during this time, an interdepartmental meeting is held at the department's offices.

- The door should never automatically lock down and deny *all* tokens entry.

Figure 2.6 shows how you would complete the time zones section of the Facility Information form to meet the needs described in the previous example. Notice, that you don't need to define a time zone for the security staff. You can assign Time Zone 9, one of the predefined time zones, to these employees' tokens to indicate that they should *always* be allowed to access the door.

Similarly, you don't need to define a time zone for the feature that automatically locks down the door. You can assign Time Zone 0, the other predefined time zone, for this feature to indicate that the feature should *never* be enabled.

[illegible]

Figure 2.6 Defining time zones and their intervals—an example

To define time zones:

1. Press \uparrow or \downarrow until you see:

>ENTER TIME ZONE FACILITY CODE

2. Press *. You see:

>TIME ZONE 1
TIME ZONE 2

3. To select Time Zone 1, press *. You see:

```
>TIME INTERVAL 1
TIME INTERVAL 2
```

4. To select Time Interval 1, press *. You see:

```
START TIME-END TIME
00:00-00:00
```

5. Type the time when the interval will start and the time when it will end. Use the 24-hour format.

For example, if the interval will start at 7:00 a.m. and end at 5:00 p.m., type **07001700**.

6. Press *. You see:

```
DAY : SMTWTFSH
(0/1) 00000000
```

7. Type **1** below the letter for each day you want to include in the interval, and type **0** below each day you want to exclude. **H** refers to the holidays you defined in Task 5.

For example, if you want the interval to include Mondays through Fridays, type **01111100**. To include only Mondays, Wednesdays, and Fridays, type **01010100**.

8. Press *. You see:

```
>TIME INTERVAL 2
TIME INTERVAL 3
```

9. For each additional time interval you want to define for the selected time zone, repeat Step 4 through Step 8.

10. When you've defined all the intervals you want for the selected time zone, press #. You see:

```
>TIME ZONE 2
TIME ZONE 3
```

11. For each additional time zone you want to define, repeat Step 3 through Step 10.

12. When you've defined all the time zones you want, press #. You see:

```
>ENTER TIME ZONE
FACILITY CODE
```

TASK 7: CHANGE THE TOKEN FORMAT (OPTIONAL)

Each V Series Magnetic Stripe Security Device and Proximity Reader Security Device is programmed at the factory to read access cards that use the following token format:

- Facility code length: 5 digits
- Facility code start location: position 2
- Card number/access code length: 6 digits
- Card number/access code start location: position 7
- Issue code length: 1 digit
- Issue code start location: position 13
- Issue code start number: 0
- Issue code end number: 0
- Look ahead setting: 0 (disabled)
- Token length: 15 digits
- Validate LRC setting: 1 (yes).

Figure 2.7 shows an example of the information generally encoded on access cards.

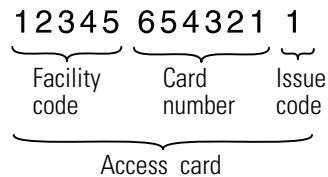


Figure 2.7 Access card

V Series Keypad Security Devices are programmed with the same default settings as magnetic stripe security devices. Usually only the following settings are relevant for keypad security devices:

- Facility code length
- Facility code start location
- Card number/access code length
- Card number/access code start location
- Token length
- Validate LRC setting.

Figure 2.8 shows an example of the information generally included in personal identification numbers (PINs).



Figure 2.8 Personal identification number (PIN)

If you want to use tokens with a different format, you can program the device to use tokens with that format.

Defining the facility code format

A facility code generally is a unique sequence of digits that is programmed into every device and encoded on every access card, or included in every PIN, that belongs to the facility. When you define the facility code format, you indicate:

- the maximum number of digits in the facility code
- the starting location of the facility code on the access cards or in the PINs.

Note: Each PIN usually consists of a facility code and an access code that uniquely identifies the user.

Defining the card number/ access code format

A card number or access code is a unique sequence of digits that identifies a user. When you define the card number or access code format, you indicate:

- the maximum number of digits in the card number or access code
- the starting location of the card number on the access cards or the access codes in the PINs.

Defining the issue code format

An issue code generally indicates how many times an access card with a particular card number has been issued. For example, when an access card is first issued to someone, it normally is encoded with Issue 1. If the access card is damaged, lost, or stolen, and a replacement card is issued to the user, the card normally would be encoded with Issue 2.

When you define the issue code format, you indicate:

- the maximum number of digits in the issue code
- the starting location of the issue code on the access cards
- the range of issue codes that the device should accept.

Note: Issue codes and the look ahead feature generally are not used for V Series Keypad Security Devices.

Using the look ahead feature

The look ahead feature lets you program a V Series Magnetic Stripe Security Device to accept an access card whose encoded issue code is

higher than the current issue code recorded for the card in the device's database. The setting for the look ahead feature determines how many numbers higher the access card's encoded issue code can be than the issue code on record for the card.

For example, if you enter 2 as the look ahead setting, the device will accept an access card whose encoded issue code is one or two numbers higher than the issue code on record for the card (as long as the issue code is within the acceptable issue code range). The device would accept an access card whose encoded issue code is 3, even if the current issue code on record for the card is 1.

When the device accepts an access card with an encoded issue code different from the current issue code on record for the card, the device automatically updates its records to reflect the encoded issue code.

A special situation can occur where the device accepts an access card with an encoded issue code lower than the current issue code on record for the card. In this situation, the device 'wraps around' when using the look ahead setting to determine whether the access card's encoded issue code is valid for the device.

For example, suppose:

- The valid issue code range is from 1 to 9.
- The look ahead setting is 1.
- The current issue code on record for card 125 is 9.
- Card 125's encoded issue code is 1.

When card 125 attempts to access the door during the time zone assigned for the access card, the device will grant access to the card. The device also will update its records to indicate that the current issue code for card 125 is 1.

Defining the token length

The token length is the total amount of information encoded on each access card or the total number of digits in each PIN.

Note: Each PIN usually consists of a facility code and an access code that uniquely identifies the user.

Determining whether to validate the LRC

You can determine whether the device validates the longitudinal redundancy check (LRC). However, always validate the longitudinal redundancy check unless a BEST representative informs you otherwise. The LRC feature is included in most token formats and helps verify that the device interprets the card data or PIN correctly.



Caution

Changing the device's token format will delete the token data already programmed for the device. If you need to change the token format, be sure to change the token format before you add facility codes and before you add tokens.

To define the facility code format:

1. Press ↑ or ↓ until you see:

```
>CONFIG SYSTEM
SET DOOR MODE
```

2. Press *. You see:

```
>COMM CARD #1
COMM CARD #2
```

3. Press ↑ or ↓ until the pointer (>) is next to **VARIABLE FORMAT**. For example, you see:

```
>VARIABLE FORMAT
RQE UNLOCK
```

4. Press *. You see:

```
ENTER PASSWORD
PASSWORD: *****
```

5. In place of the asterisks, type the communication token password.

6. To select facility code, press *. You see:

```
>FACILITY CODE
CARD NUMBER
```

7. Press *. You see:

```
>FC LENGTH
FC LOCATION
```

8. Press *. You see:

```
>FC LENGTH
5 (0-9)
```

9. Type the maximum number of digits (from 0 to 9) in the facility codes for this token format. For example, if the maximum facility code length is four digits, type **4**.

If you type **0**, the device will not check the facility code when determining whether to grant access to a token.

10. Press *. You see:

```
>FC LOCATION
FC LENGTH
```

11. Press *. For example, you see:

```
>FC LOCATION
02 (01-99)
```

(If you set the facility code length to 0 in Step 9, you see **NO DATA REQUIRED**. Skip Step 12.)

12. Type the starting location of the facility code (from 1 to 99), preceded by a zero if necessary. For example, if the facility code starts at position 3, type **03**.
13. Press *. You see:

```
>FC LENGTH
FC LOCATION
```

14. Press #. You see:

```
>CARD NUMBER
ISSUE CODE
```

Now you're ready to define the card number or access code format by following the steps in the next section.

To define the card number or access code format:

1. To select card number, press *. You see:

```
>CARD # LENGTH
CARD # LOCATION
```

2. Press *. You see:

```
>CARD # LENGTH
6 (1-9)
```

3. Type the maximum number of digits (from 1 to 9) in the card number or access code for this token format.

4. Press *. You see:

```
>CARD # LOCATION
CARD # LENGTH
```

5. Press *. You see:

```
>CARD # LOCATION
07 (01-99)
```

6. Type the starting location of the card number or access code (from 1 to 99), preceded by a zero if necessary.

7. Press *. You see:

```
>CARD # LENGTH
CARD # LOCATION
```

8. Press #. You see:

```
>ISSUE CODE
CARD LENGTH
```

Now you're ready to define the issue code format by following the steps in the next section.

Note: Issue codes and the look ahead feature generally are not used for V Series Keypad Security Devices. If you are changing the token format for a keypad security device, you generally can skip the steps in the following section, *To define the issue code format* and in the section *To define the look ahead feature*. Instead, press ↑ or ↓ until you see:

```
>CARD LENGTH
VALIDATE LRC
```

Then, follow the instructions in the section *To define the token length* (see [page 2-26](#)).

To define the issue code format:

1. To select issue code, press *. You see:

```
>IC LENGTH
IC LOCATION
```

2. Press *. You see:

```
>IC LENGTH
1 (0-4)
```

3. Type the maximum number of digits (from 0 to 4) in the issue code for this token format. If you type **0**, the device will not check the issue code when determining whether to grant access to a token.
4. Press *. You see:

```
>IC LOCATION
START #
```

5. Press *. For example, you see:

```
>IC LOCATION
13 (01-99)
```

(If you set the issue code length to 0 in Step 3, you see **NO DATA REQUIRED**. Skip Step 6.)

6. Type the starting location of the issue code (from 1 to 99), preceded by a zero if necessary.
7. Press *. You see:

```
>START #
END #
```

8. Press *. For example, you see:

```
>START #
0
```

(If you set the issue code length to 0 in Step 3, you see **NO DATA REQUIRED**. Skip Step 9.)

9. Type the lowest-numbered issue code that the device should accept, preceded by enough zeros to replace the digits you see (the total number of digits in the issue code for the selected token format). The device will reject any tokens with issue codes lower than this number.

For example, if the device should reject any token with an issue number *lower than* 4 and the issue code for the selected token format has one digit, type **4**.

10. Press *. You see:

```
>END #
LOOK AHEAD
```

11. Press *. For example, you see:

```
>END #
0
```

(If you set the issue code length to 0 in Step 3, you see **NO DATA REQUIRED**. Skip Step 12.)

12. Type the highest-numbered issue code that the device should accept, preceded by enough zeros to replace the digits you see (the total number of digits in the issue code for the selected token format). The device will reject any tokens with issue codes higher than this number.

For example, if the device should reject any token with an issue number *higher than* 8 and the issue code for the selected token format has one digit, type **8**.

13. Press *. You see:

```
>LOOK AHEAD
IC LENGTH
```

Now you're ready to define the look ahead feature by following the steps in the next section.

To define the look ahead feature:

1. To select look ahead, press *. For example, you see:

```
>LOOK AHEAD
0
```

(If you set the issue code length to 0 in Step 3 in the section *Defining the issue code format* on [page 2-19](#), you see **NO DATA REQUIRED**. Skip Step 2.)

2. Type the setting that determines whether a valid token with an issue number different from the issue number currently on record for that token can access the door. Type enough zeros before the setting to replace the digits you see (the total number of digits in the issue code for the selected token format). For more information, see *Using the look ahead feature* on page 2-19.

For example, if the device should accept a token with an issue number up to three numbers higher than the current issue number on record for that token, type **3** in this field.

3. Press *. You see:

```
>IC LENGTH
IC LOCATION
```

4. Press #. You see:

```
>CARD LENGTH
VALIDATE LRC
```

Now you're ready to define the token length by following the steps in the next section.

To define the token length:

1. Press *. You see:

```
>CARD LENGTH
15 (01-99)
```

2. Type the total number of digits of data (from 1 to 99) on the access cards or in the PINs, preceded by a zero if necessary. For example, if there are 20 digits of data on the access cards or in the PINs, type **20**.
3. Press *. You see:

```
>VALIDATE LRC
FACILITY CODE
```

Now you're ready to define the validate LRC feature by following the steps in the next section.

To define the validate LRC feature:

1. Press *. You see:

```
>VALIDATE LRC
0=NO 1=YES: 1
```

2. If the device should validate the longitudinal redundancy check (LRC), type **1**. If the device should not validate the LRC, type **0**.

Note: For V Series Keypad Security Devices, always type **1**.

3. Press *. You see:

```
>FACILITY CODE
CARD NUMBER
```

4. Press #. You see:

```
UPDATE VAR FORMAT
0=NO 1=YES: 0
```

5. To save the token format you've defined, type **1**.

Note: If the token format settings do not make sense, you see **INVALID VCF DATA**. For example, this message appears if the length of one item makes the location defined for another item impossible. Review the settings to find the error.

6. Press *. For example, you see:

```
>VARIABLE FORMAT
RQE UNLOCK
```


7. Press #. You see:

```
>CONFIG SYSTEM
SET DOOR MODE
```

TASK 8: ADD FACILITY CODES

So that the V Series Security Device can verify the facility code on access cards or included in personal identification numbers (PINs), you need to add the facility codes you want the device to accept. You also need to define the range of card numbers or access codes that is acceptable for each facility code. The device will reject card numbers or access codes outside this range. Use the information you provided on the Facility Information form in Task 1 (see [page 2-3](#)).

What is a facility code?

A facility code generally is a unique sequence of digits that is programmed into every device and encoded on every access card, or included in every PIN, that belongs to the facility. The facility code helps ensure the security of a facility's devices since an access card or PIN without the facility code can't open a door even if the card has a valid card number or the PIN has a valid access code.

You can program a device with up to eight facility codes, although in most cases only one facility code is needed. However, if you add multiple facility codes, the range of valid card numbers or access codes for one facility code normally shouldn't overlap with the range of valid card numbers or access codes for another facility code. If a device's user database includes access cards with the same card number or PINs with the same access code, you can't be certain which user is associated with events recorded in the device's history for this card number or access code.

For example, you could define the following facility codes and card number or access code ranges.

Facility Code	Starting Card No. or Access Code	Ending Card No. or Access Code
12345	1	199
54321	200	299
13579	300	399

To add a facility code:

1. Press ↑ or ↓ until you see:

```
>FACILITY CODE  
CONFIG SYSTEM
```

2. Press *. For example, you see:

```
>FC 01 99999  
FC 02 00000
```

3. To select facility code 1, press *. For example, you see:

```
>FC 01 99999  
CODE: 99999
```

4. Type the facility code, preceded by enough zeros to replace the digits you see (the total number of digits in the facility code for the selected token format). For example, if the facility code is 12345 and the facility code for the selected token format has five digits, type **12345**.

5. Press *. For example, you see:

```
FC 01 75501  
S-CARD# 000001
```

6. Type the lowest card number or access code (with the facility code entered in Step 4) that the device should accept. Type enough zeros before the card number or access code to replace the digits you see (the total number of digits in the card number or access code for the selected token format). The device will reject any tokens with card numbers or access codes lower than this number.

For example, if the lowest card number or access code for this facility is 1 and the card number or access code for the selected token format has six digits, type **000001**.

7. Press *. For example, you see:

```
FC 01 75501  
E-CARD# 999998
```

8. Type the highest card number or access code (with the facility code entered in Step 4) that the device should accept. Type enough zeros before the card number or access code to replace the digits you see (the total number of digits in the card number or access code for the selected token format). The device will reject any tokens with card numbers or access codes higher than this number.

For example, if the highest card number or access code for this facility is 999 and the card number or access code for the selected token format has six digits, type **000999**.

9. Press *. You see:

```
>FC 02 00000
FC 03 00000
```

10. For each additional facility code you want to add, repeat Step 3 through Step 9.
11. When you've finished adding facility codes, press #. You see:

```
>FACILITY CODE
CONFIG SYSTEM
```



Caution

When you add the facility code for the device, the temporary communication token is disabled. Be sure to perform Task 12 to add a permanent communication token before you end communications or before the device exits communication mode after 5 minutes of inactivity. Otherwise you will be locked out of the device. If you get locked out of the device, see the V Series Service Manual, Emergency Operations section.

TASK 9: DEFINE V SERIES CONTROLLER FEATURES (CONTROLLER ONLY)

If you are programming a V Series Controller, you need to define special features available only for controllers. To define these features, you:

- select a RQE unlock setting
- select a remote unlock device setting
- select the door contact type
- define the door open too long feature
- select the door forced alarm setting
- select the alarm output duration.

When defining controller features, use the information you provided on the Token & Door Information form or the Token by Door Information form (see [page 2-3](#)).

Using the RQE unlock feature

The controller can accept a request-to-exit signal from a lock or a separate request-to-exit device, such as a button, can be connected to a controller. When someone turns a door knob with a request-to-exit feature, or presses a request-to-exit button, the controller does not trigger an alarm when the door is opened. If the controller is programmed for the RQE unlock feature, the controller also unlocks the door. The RQE unlock feature is used to let people out of an area secured by a lock that remains locked all the time, such as a magnetic lock. By default, the RQE unlock feature is turned off.

Using the remote unlock feature

A remote unlock device, such as a button, can be connected to a controller. This device can be located away from the door. When someone, such as a receptionist, presses the remote unlock button, the controller unlocks the door if the controller is programmed for the remote unlock feature. By default, the remote unlock feature is turned off.

Selecting the door contact type

You need to indicate whether the door contact for the controller is normally closed or normally open. By default, the door contact setting is normally open.

Defining the door open too long feature

You can program the controller to monitor whether the door has not latched because it did not close correctly or because it has been propped open. This feature helps maintain the security of the area that the door provides access to. For example, if the default settings are used, the following events take place.

Suppose the controller has granted access to someone who enters the secured area and props open the door. For 30 seconds after the end of the unlock duration nothing happens. This period is called the delay duration. It provides time for the person granted access to enter the secured area and close the door.

If the door remains open at the end of the delay duration, the reader connected to the controller triggers a local alarm (if equipped to do so, the reader sounds the alarm and flashes its red LED), warning people nearby that the door is open. If the door remains open, the local alarm continues for 60 seconds. This time period is called the warning duration.

If the door remains open at the end of the warning duration, the controller activates its alarm output. If the door remains open, the controller continues to activate its alarm output for 60 seconds.

When you select the door open too long feature for the controller, you can change:

- the delay duration
- the warning duration
- the alarm duration.

You also can eliminate one or two of these durations. For example, if you want a local warning alarm to begin to sound as soon as the unlock duration ends, you can change the delay duration to 0.

Selecting the door forced alarm feature

You need to indicate whether the controller should trigger an alarm when the door controlled by the controller is opened without use of a valid access method. When the controller triggers a door forced alarm, the controller's alarm output is activated for the number of seconds selected for the alarm output duration. By default, the door forced alarm feature is turned off.

Note: An alerting device, such as a siren or strobe light, or a security system generally is connected to the controller's alarm output.

Selecting the alarm output duration

The default alarm output duration is 120 seconds. When the controller triggers a door forced alarm or a tamper alarm, it activates its alarm output for 120 seconds. You can change this duration.

To define the RQE unlock feature:

1. Press ↑ or ↓ until you see:

```
>CONFIG SYSTEM
SET DOOR MODE
```

2. Press *. You see:

```
>COMM CARD #1
COMM CARD #2
```

3. Press ↑ or ↓ until you see:

```
>RQE UNLOCK
REMOTE UNLOCK
```

4. Press *. You see:

```
>RQE UNLOCK
0=NO 1=YES: 0
```

5. If you want the controller to use the RQE unlock feature, type **1**.
If you do not want the controller to use the RQE unlock feature, type **0**.

6. Press *. You see:

```
>REMOTE UNLOCK  
DOOR STATUS
```

Now you're ready to define the remote unlock feature by following the steps in the next section.

To define the remote unlock feature:

1. To select remote unlock, press *. You see:

```
>REMOTE UNLOCK  
0=NO 1=YES: 0
```

2. If you want the controller to use the remote unlock feature, type **1**.
If you do not want the controller to use the remote unlock, type **0**.

3. Press *. You see:

```
>DOOR STATUS  
ALARM OUTPUT
```

Now you're ready to define the door status features by following the steps in the next section.

To define the door status features:

1. To select door status, press *. You see:

```
>DOOR CONTACT  
DOTL
```

2. To select door contact, press *. You see:

```
>DOOR CONTACT  
0=NO 1=YES: 0
```

3. If the door contact connected to the controller is normally closed, type **1**.
If the door contact connected to the controller is normally open, type **0**.

4. Press *. You see:

```
>DOTL  
DOOR FORCED
```

5. To select DOTL, press *. You see:

```
>DOTL ENABLE  
DELAY DURATION
```

6. To select DOTL enable, press *. You see:

```
>DOTL ENABLE
0=NO 1=YES: 1
```

7. If the controller uses the door open too long feature, type **1**.
If the controller does not use the door open too long feature, type **0**.
8. Press *. You see:

```
>DELAY DURATION
WARN DURATION
```

9. To select delay duration, press *. You see:

```
>DELAY DURATION
030 (SEC)
```

(If you set the DOTL enable feature to 0 in Step 7, you see **NO DATA REQUIRED**. Skip Step 10.)

10. Type the number of seconds (from 1 to 999) the controller should wait after the unlock duration ends before triggering a local alarm, preceded by zeros if necessary. For example, if the controller should wait 60 seconds, type **060**.

To indicate no delay, type **000**.

11. Press *. You see:

```
>WARN DURATION
ALARM DURATION
```

12. To select warning duration, press *. You see:

```
>WARN DURATION
060 (SEC)
```

(If you set the DOTL enable feature to 0 in Step 7, you see **NO DATA REQUIRED**. Skip Step 13.)

13. Type the number of seconds (from 1 to 998) a local warning alarm should sound, preceded by zeros if necessary. For example, if the local alarm should sound for two minutes, type **120**.

To indicate that no local warning alarm should sound (at the end of the delay duration a remote alarm is triggered), type **000**.

To indicate that the local warning alarm should sound until the door is closed (no remote alarm is triggered), type **999**.

14. Press *. You see:

```
>ALARM DURATION
DOTL ENABLE
```

15. To select alarm duration, press *. You see:

```
>ALARM DURATION
060 (SEC)
```

(If you set the DOTL enable feature to 0 in Step 7, you see **NO DATA REQUIRED**. Skip Step 16.)

16. Type the number of seconds (from 1 to 998) the controller should activate its alarm output for a door open too long alarm, preceded by zeros if necessary. For example, if the controller should activate its alarm output for 90 seconds, type **090**.

To indicate that the remote alarm should continue until the door is closed, type **999**.

17. Press *. You see:

```
>DOTL ENABLE
DELAY DURATION
```

18. Press #. You see:

```
>DOOR FORCED
DOOR CONTACT
```

19. To select door forced, press *. You see:

```
>DOOR FORCED
0=NO 1=YES: 0
```

20. If the controller should trigger door forced alarms, type **1**.
If the controller should not trigger door forced alarms, type **0**.

21. Press *. You see:

```
>DOOR CONTACT
DOTL
```

22. Press #. You see:

```
>ALARM OUTPUT
COMM CARD #1
```

Now you're ready to select the alarm output duration by following the steps in the next section.

To select the alarm output duration:

1. To select alarm output, press *. You see:

```
>ALARM OUTPUT
121      (SEC)
```

2. Type the number of seconds (from 1 to 998) the controller should activate its alarm output for a door forced alarm or a tamper alarm, preceded by zeros if necessary. For example, if the controller should activate its alarm output for 60 seconds, type **060**.

To indicate that the controller should activate its alarm output for .5 seconds, type **000**.

To indicate that the alarm output should remain activated until the alarm condition no longer exists, type **999**.

3. Press *. You see:

```
>COMM CARD #1
COMM CARD #2
```

4. Press #. You see:

```
>CONFIG SYSTEM
SET DOOR MODE
```

TASK 10: SET THE CHASSIS TYPE (ELECTRONIC LOCK ONLY)

If you are programming a V Series Electronic Lock (not a controller), you need to identify the lock chassis type (cylindrical or mortise) so the electronic lock is programmed to operate its motor for the appropriate duration when operating the lock. The cylindrical motor is required to run slightly longer than the mortise motor.

Note: Cylindrical chassis types have a figure-eight core in the knob or lever. Mortise chassis types have a figure-eight core in the escutcheon or none at all. By default, the lock chassis type is programmed as cylindrical. You can skip this task if the electronic lock has a cylindrical chassis.

To set the chassis type:

1. Press ↑ or ↓ until you see:

```
>CHASSIS TYPE
VIEW DATA BASE
```

2. Press *. You see:

```
>CYLINDRICAL
MORTISE
```

3. Press ↑ or ↓ until the pointer (>) is next to the type of chassis you want to select.
4. Press *. You see:

>CHASSIS TYPE
VIEW DATA BASE

TASK 11: PROGRAM TIMED ACCESS FEATURES

You need to program the unlock duration for the V Series Security Device—the number of seconds that the door remains unlocked when accessed by a token. You can also select time zones for three timed access features:

- **Door lock time zone.** This feature lets you select a time zone when the door automatically locks down, denying *all* tokens access, and then later resumes normal operation.
- **Facility code only time zone.** This feature lets you select a time zone when all tokens with a valid facility code can access the door.
- **Door unlock time zone.** This feature lets you select a time zone when the lock automatically unlocks (or unlocks when a valid token accesses the door) and then later relocks.

You determine when each timed access feature is in effect by assigning one of the time zones you defined in Task 6, or one of the predefined time zones, to the feature. If you want a timed access feature never to be in effect, assign Time Zone 0. If you want a timed access feature always to be in effect, assign Time Zone 9.

If any time zones you assign for timed access features overlap, the most secure feature is in effect, according to the priority listed below. For example, if the time zone selected for the door unlock feature overlaps the time zone selected for the door lock feature, the door lock feature is in effect when the time zones overlap.

1. Door lock time zone
2. Facility code only time zone
3. Door unlock time zone

When programming timed access features, use the information you provided on the Token & Door Information form or the Token by Door Information form in Task 1 (see [page 2-3](#)).

Setting the unlock duration

Unlock duration is the programming function that determines how long the door controlled by the device remains unlocked when accessed by a token. By default, the unlock duration is 3 seconds.

To set the unlock duration:

1. Press ↑ or ↓ until you see:

```
>CONFIG READER
  ADD/MODIFY CARD
```

2. Press *. You see:

```
>UNLOCK DURATION
  DOOR LOCK TZ
```

3. Press *. You see:

```
>UNLOCK DURATION
  03      (SEC)
```

4. Type the number of seconds that you want the door to remain unlocked when accessed by a token, preceded by a zero if necessary. For example, if you want the door to unlock for five seconds, type **05**.

To indicate .5 seconds, type **00**.

Note: If you are programming a controller, the range for the unlock duration is 0 to 99. If you are programming an electronic lock, the range is 3 to 99.

5. Press *. You see:

```
>DOOR LOCK TZ
  FC-CODE ONLY TZ
```

6. Press #. You see:

```
>CONFIG READER
  ADD/MODIFY CARD
```

**Selecting the
door lock time
zone**

Use the door lock feature to program regular time periods when you don't want anybody to be able to access the door. The only way to access a door when the door lock feature is in effect is with the communication token (or by key). By default, the door lock time zone is 0 (never).

To set the device for timed automatic lock down:

1. Press ↑ or ↓ until you see:

```
>CONFIG READER  
ADD/MODIFY CARD
```

2. Press *. You see:

```
>UNLOCK DURATION  
DOOR LOCK TZ
```

3. Press ↑ or ↓ until you see:

```
>DOOR LOCK TZ  
FC-CODE ONLY TZ
```

4. Press *. You see:

```
>DOOR LOCK TZ  
0      (0-9)
```

5. Type the number of the time zone representing the time periods when you want the lock down feature to be in effect. Type the number of one of the time zones you defined in Task 6 (from **1** to **8**), or type **0** for never.

For information about defining time zones, see [page 2-14](#).

6. Press *. You see:

```
>FC-CODE ONLY TZ  
DOOR UNLOCK TZ
```

7. Press #. You see:

```
>CONFIG READER  
ADD/MODIFY CARD
```

Selecting the facility code only time zone

Use the facility code only feature to program regular time periods when you want anyone with a token that has a valid facility code to be able to access the door. This feature generally is used for a device that protects a common entry point to a building or area where many people need access. Since you can program no more than 1000 tokens to access a door, you can also use this feature when more than 1000 tokens need to access a door.

For example, you could let all users with tokens that have a valid facility code access a door at the main entrance to a building during normal business hours, such as on Mondays through Saturdays, from 8:00 a.m. to 10:00 p.m.

By default, the facility code only time zone is 0 (never).



Caution

If someone loses an access card, the card can be used to access the door during the facility code only time zone. To prevent the card from being used to access the door, you can disable the facility code only time zone, or you can change the facility code for the door and all of the cards that access it.

To set the lock for timed facility code only operation:

1. Press ↑ or ↓ until you see:

```
>CONFIG READER
  ADD/MODIFY CARD
```

2. Press *. You see:

```
>UNLOCK DURATION
  DOOR LOCK TZ
```

3. Press ↑ or ↓ until you see:

```
>FC-CODE ONLY TZ
  DOOR UNLOCK TZ
```

4. Press *. You see:

```
>FC-CODE ONLY TZ
  0      (0-9)
```

5. Type the number of the time zone representing the time periods when you want the facility code only feature to be in effect. Type the number of one of the time zones you defined in Task 6 (from **1** to **8**), or type **0** for never, or type **9** for always.

For information about defining time zones, see [page 2-14](#).

6. Press *. You see:

```
>DOOR UNLOCK TZ
  UNLOCK DURATION
```

7. Press #. You see:

```
>CONFIG READER
  ADD/MODIFY CARD
```

Selecting the door unlock time zone

Use the door unlock feature to program regular time periods when you want the door to unlock and then later relock. You can determine whether the door automatically unlocks at the start of a door unlock time interval or whether the door unlocks only when accessed by a valid token.

For example, you can use the door unlock feature for devices that protect conference room doors that you want to remain closed, but unlocked, for selected time periods. If you don't enable the first card unlock feature, the doors automatically unlock at the start of a door unlock time interval. The doors remain unlocked until the end of the door unlock time interval.

You might use the door unlock feature and the first card unlock feature for the doors at the front of a building. For example, suppose you'd like the doors to unlock at 8:00 a.m. on Mondays through Fridays, but only if someone has arrived. You would also like the doors to relock at 5:00 p.m. each day. For the door unlock time zone, you can assign a time zone defined to start at 8:00 a.m. and end at 5:00 p.m. on Mondays through Fridays. You can also enable the first card unlock feature.

If the first valid token to access the door doesn't do so until 8:15 a.m., the door remains locked until 8:15 a.m. and then unlocks when accessed by the valid token. If no valid token accesses the door on a particular day, the door remains locked all day.

By default, the door unlock time zone is 0 (never). By default, the first card unlock feature is disabled.

To set the lock for timed unlocking:

1. Press ↑ or ↓ until you see:

```
>CONFIG READER  
ADD/MODIFY CARD
```

2. Press *. You see:

```
>UNLOCK DURATION  
DOOR LOCK TZ
```

3. Press ↑ or ↓ until you see:

```
>DOOR UNLOCK TZ  
UNLOCK DURATION
```

4. Press *. You see:

```
>DOOR UNLOCK TZ  
0      (0-9)
```

5. Type the number of the time zone representing the time periods when you want the door unlock feature to be in effect. Type the number of one of the time zones you defined in Task 6 (from **1** to **8**), or type **0** for never.

For information about defining time zones, see [page 2-14](#).

6. Press *. You see:

```
>1ST CARD UNLOCK
0=NO 1=YES: 0
```

7. If you want the door to unlock only when accessed by a valid token, type **1**.

If you want the door to unlock automatically at the start of a door unlock time interval, type **0**.

8. Press *. You see:

```
>UNLOCK DURATION
DOOR LOCK TZ
```

9. Press #. You see:

```
>CONFIG READER
ADD/MODIFY CARD
```

TASKS TO DEFINE THE USER DATABASE

This section describes the following tasks, which you perform to define the V Series Security Device's user database:

Task 12: Add a communication token and password. See [page 2-41](#).

Task 13: Add tokens. See [page 2-43](#).

Task 14: Delete the temporary operator token. See [page 2-46](#).

Task 15: Add a range of access cards (optional—magnetic stripe security device or proximity security device only).
See [page 2-46](#).

Task 16: Verify the user database. See [page 2-48](#).

TASK 12: ADD A COMMUNICATION TOKEN AND PASSWORD

You need to add a permanent communication token to replace the temporary communication token used to access the V Series Security Device for initial programming. The permanent communication token lets you access the device at any time to program it. The same permanent communication token generally is used for all the devices in your system.

You must add *at least one* communication token and you can have a maximum of two. You pick the password you want to use for each communication token. The password can be between one and six digits. Use the information you provided on the Facility Information form in Task 1 (see [page 2-3](#)).



You must remember the communication token's password to access the device. If you can't remember the password, you must manually reset the device's electronic circuit board following the instructions in the V Series Service Manual, Emergency Operations section.

To add a communication token and password:

1. Press ↑ or ↓ until you see:

```
>CONFIG SYSTEM  
SET DOOR MODE
```

2. Press *. You see:

```
>COMM CARD #1  
COMM CARD #2
```

3. To select comm card #1, press *. For example, you see:

```
>COMM CARD #1  
999999
```

4. Type the card number or access code for the communication token, preceded by enough zeros to replace the digits you see (the total number of digits in the card number or access code for the selected token format). For example, if the card number or access code is 125 and the card number or access code for the selected token format has six digits, type **000125**.

5. Press *. You see:

```
COMM PASSWORD #1  
PASSWORD: 123456
```

6. In place of the default password, type the password for the communication token (from 1 to 6 digits), preceded by enough zeros to total six digits. For example, if the password is 678, type **000678**. When you enter the password using the handheld terminal's keypad to access the device, you would type **678**.

7. Press *. You see:

```
>COMM CARD #2  
VARIABLE FORMAT
```

8. To add a second communication token, repeat Step 3 through Step 7.

9. When you've finished adding communication tokens, press #. You see:

```
>CONFIG SYSTEM
SET DOOR MODE
```

TASK 13: ADD TOKENS

You need to add the tokens that need access to the door to the V Series Security Device's user database. For each token that needs access to the door, you need to enter:

- the card number or access code
- the issue code
- the time zone representing the time periods when you want the token to be able to access the door
- the expiration date
- the issue code
- the deadbolt override setting
- the passage mode setting.

Note: Issue codes generally are not used for V Series Keypad Security Devices.

When adding tokens, use the information you provided on the Token & Door Information form or the Token by Door Information form in Task 1 (see [page 2-3](#)).

Assigning the time zone

For each token you add for the device, you assign a time zone representing the time periods when you want the token to be able to access the door. You can select one of the time zones you defined in Task 6, or one of the predefined time zones. If you want a token never to be able to access a door, assign Time Zone 0. If you want a token always to be able to access a door, assign Time Zone 9.

For information about defining time zones, see [page 2-14](#).

Setting deadbolt override

If you grant the deadbolt override privilege to a token, the token can access the door controlled by an electronic lock even when the door's deadbolt is thrown.

Note: The deadbolt override feature applies only to electronic locks with a mortise deadbolt function chassis.

Setting passage mode

When a user with the passage mode privilege for a device uses his or her token, hears the door unlock, and uses his or her token again within the unlock duration, the door will remain unlocked. This feature can be used only during the time zone assigned to the token.

When the door is unlocked using the passage mode feature, the door remains unlocked until someone with the passage mode privilege locks the door, or until a door lock time interval begins or a facility code only time interval begins. If you give tokens the passage mode privilege, you might want to define a brief door lock time interval at the end of each work day to make sure the door is relocked. For more information, see *Selecting the door lock time zone* on page 2-37.

Similarly, if the user uses his or her token when the door is in passage mode, the user can relock the lock by using his or her token again within the unlock duration. This feature can be used at any time although it does not relock a door during a door unlock time zone.

For information about setting the unlock duration, see [page 2-36](#).

Tip: Instead of entering his or her PIN twice to use the passage mode feature at a V Series Keypad Security Device, a user can enter his or her PIN, press *, then press #.

Note: To add a range of consecutively numbered access cards, see [page 2-46](#).

To add a token:

1. Press ↑ or ↓ until you see:

>ADD/MODIFY CARD
DELETE CARD

2. Press *. For example, you see:

ENTER CARD #
000000

3. Type the token's card number or access code, preceded by enough zeros to replace the zeros you see (the total the number of digits in the card number or access code for the selected token format). For example, if the card number or access code is 123 and the card number or access code for the selected token format has six digits, type **000123**.

4. Press *. For example, you see:

ENTER ISSUE CODE
0 (0-9)

5. Type the token's issue code, preceded by enough zeros to replace the zeros you see (the total number of digits in the issue code for the selected token format). For example, if the issue code is 2 and the issue code for the selected token format has one digit, type **2**.

Note: Issue codes generally are not used for V Series Keypad Security Devices.

6. Press *. You see:

ENTER TZ #
0 (0-9)

7. Type the number of the time zone representing the time periods when you want the token to be able to access the door. Type the number of one of the time zones you defined in Task 6 (from **1** to **8**), or type **0** for never, or type **9** for always.

For information about defining time zones, see [page 2-14](#).

8. Press *. You see:

EXPIRE: YY/MM/DD
DATE: 00/00/00

9. Type the date when you want the token to expire and no longer be able to access the door. Type the year, then the month, then the day.

For example, if you want the token to expire on December 31, 2001, type **011231**.

10. Press *. You see:

BOLT OVERRIDE
0=NO 1=YES: 1

11. To give the token the deadbolt override privilege, type **1**. If you do not want to give the token the deadbolt override privilege, type **0**.

For information about this feature, see [page 2-43](#).

Note: The deadbolt override feature applies only to electronic locks with a mortise deadbolt function chassis.

12. Press *. You see:

PASSAGE MODE
0=NO 1=YES: 0

13. To give the token the passage mode privilege, type **1**. If you do not want to give the token the passage mode privilege, type **0**.

For information about this feature, see [page 2-43](#).

14. Press *. You see:

>ADD/MODIFY CARD
DELETE CARD

TASK 14: DELETE THE TEMPORARY OPERATOR TOKEN

When you changed the V Series Security Device's facility code from the factory default setting in Task 8 (see [page 2-18](#)), you disabled the temporary operator token. To keep the device's database accurate and up-to-date, you need to delete the temporary operator token from the device's user database.

To delete the temporary operator token:

1. Press ↑ or ↓ until you see:

>DELETE CARD
ADD CARD RANGE

2. Press *. For example, you see:

ENTER CARD #
000000

3. Type **999998**, the card number or access code for the temporary operator token.
4. Press *. The token is deleted. You see:

>DELETE CARD
ADD CARD RANGE

TASK 15: ADD A RANGE OF ACCESS CARDS (OPTIONAL—MAGNETIC STRIPE SECURITY DEVICE OR PROXIMITY SECURITY DEVICE ONLY)

You can add a range of access cards with consecutive card numbers that need access to the door controlled by the device. All access cards in the range will have the same:

- issue code
- time zone setting
- expiration date
- deadbolt override setting
- passage mode setting.

When adding a range of access cards, use the information you provided on the Token & Door Information form or the Token by Door Information form in Task 1 (see [page 2-3](#)).

Note: This feature generally is not used for V Series Keypad Security Devices since the use of consecutive access codes can compromise the security of your access control system.

To add a range of access cards:

1. Press ↑ or ↓ until you see:

>ADD CARD RANGE
DEL CARD RANGE

2. Press *. For example, you see:

STARTING CARD #
000000

3. Type the lowest card number in the range, preceded by enough zeros to replace the zeros you see (the total number of digits in the card number for the selected token format). For example, if the lowest card number is 101 and the card number for the selected token format has six digits, type **000101**.

4. Press *. For example, you see:

ENDING CARD #
000000

5. Type the highest card number in the range, preceded by enough zeros to replace the zeros you see. For example, if the highest card number is 199, type **000199**.

6. Press *. For example, you see:

ENTER ISSUE CODE
0 (0-9)

7. Type the issue code for the access cards in the range, preceded by enough zeros to replace the zeros you see (the total number of digits in the issue code for the selected token format). For example, if the issue code is 2 and the issue code for the selected token format has one digit, type **2**.

8. Press *. You see:

ENTER TZ #
0 (0-9)

9. Type the number of the time zone representing the time periods when you want the access cards in the range to be able to access the door. Type the number of one of the time zones you defined in Task 6 (from **1** to **8**), or type **0** for never, or type **9** for always.

For information about defining time zones, see [page 2-14](#).

10. Press *. You see:

EXPIRE: YY/MM/DD
DATE: 00/00/00

11. Type the date when you want the access cards in the range to expire and no longer be able to access the door. Type the year, then the month, then the day.

For example, if you want the cards to expire on April 15, 2001, type **010415**.

12. Press *. You see:

BOLT OVERRIDE
0=NO 1=YES: 1

13. To give the access cards in the range the deadbolt override privilege, type **1**. If you do not want to give the access cards the deadbolt override privilege, type **0**.

For information about this feature, see [page 2-43](#).

Note: The deadbolt override feature applies only to electronic locks with a mortise deadbolt function chassis.

14. Press *. You see:

PASSAGE MODE
0=NO 1=YES: 0

15. To give the access cards in the range the passage mode privilege, type **1**. If you do not want to give the access cards the passage mode privilege, type **0**.

For information about this feature, see [page 2-43](#).

16. Press *. You see:

>ADD CARD RANGE
DEL CARD RANGE

TASK 16: VERIFY THE USER DATABASE

When you've finished selecting programming settings and defining the user database for the device, you should review the tokens you added to the device to make sure the information is correct.

Tip: If you need to change the information for one of the tokens, follow the instructions in the section *Modifying tokens* on [page 3-2](#).

To view the token database:

1. Press ↑ or ↓ until you see:

```
>VIEW DATA BASE
RESET SYSTEM
```

2. Press *. You see:

```
>VIEW HISTORY
VIEW CARD DATA
```

3. Press ↑ or ↓ until you see:

```
>VIEW CARD DATA
VIEW SYS DATA
```

4. Press *. You see the total number of tokens in the device's database, for example:

```
>VIEW CARD DATA
TOTAL CARD # 0200
```

5. Press *. You see the lowest card number or access code in the device's database, for example:

```
STARTING CARD #
000001
```

6. To view the user database starting with the lowest card number or access code, press *. To view the user database starting with a specific card number or access code, type the card number or access code you want and press *.

For example, you might type **000101** and see:

Card number or access code	Issue code		
<pre>CARD 000101 1 TZ3 01/12/31 DB1 P0</pre>			
Time zone	Expiration date	Deadbolt override privilege setting	Passage mode privilege setting

7. Press ↑ or ↓ to continue viewing the tokens in the database.
8. When you've finished viewing tokens in the database, press # twice.
You see:

>VIEW DATA BASE
RESET SYSTEM

FINAL TASK

This section describes the following task, which you perform when you've finished programming the device:

Task 17: Disconnect the handheld terminal. See [page 2-50](#).

TASK 17: DISCONNECT THE HANDHELD TERMINAL

When all user information has been confirmed and you've finished programming the V Series Security Device, you can close communication with the device and disconnect the handheld terminal.

To disconnect the handheld terminal:

1. Press # until you see:

CLOSE COMMUNICA-
TION
ARE YOU SURE?

2. Press *. You see:

COMMUNICATION
IS CLOSED

3. Press the handheld's **ON/OFF** button.
4. Unplug the handheld-to-device cable from the device.
5. If you programmed a V Series Controller, place DIP switch 4 on the controller board in the OFF position.

PROGRAMMING OTHER V SERIES SECURITY DEVICES

Repeat Task 3 through Task 17 for every V Series Security Device until all devices are programmed.

3

HOW DO I MAINTAIN THE V SERIES SYSTEM?

To maintain the V Series System, you need to keep each V Series Security Device's programming up to date. You might need to modify a device's programming to change how it operates. You also might need to add, modify, or delete information in a device's user database.

To make one of the following changes to a device's programming settings or user database, see the indicated page:

- changing or adding holidays. See [page 2-13](#)..
- changing or adding a time zone. See [page 2-16](#)..
- adding a facility code or changing the range of card numbers or access codes for a facility code. See [page 2-28](#)..
- changing or adding a communication token and password. See [page 2-42](#)..
- changing timed access features. See [page 2-36](#)..
- changing the user database. See [page 3-9](#)..

This chapter also provides instructions for performing the following activities:

- programming a device to override time zone control. See [page 3-6](#)..
- viewing a device's history. See [page 3-9](#)..
- viewing a device's system data. See [page 3-10](#)..
- resetting a device. See [page 3-10](#)..
- clearing an electronic lock's low battery message. See [page 3-12](#)..

To perform any of the activities described in this chapter for a V Series Security Device, the handheld terminal must be in communication with the device. For instructions, see [page 2-9](#). When you've finished performing activities at the device, you can close communication with the device and disconnect the handheld. For instructions, see [page 2-50](#).

CHANGING A V SERIES SECURITY DEVICE'S USER DATABASE

A V Series Security Device's user database describes all of the tokens that can access the device. When maintaining the user database for a device, you can:

- add tokens
- modify tokens
- delete tokens
- add a range of access cards
- delete a range of access cards.

It's easier to change the user database if you first complete a Token & Door Information form or a Token by Door Information form (see [page 2-3](#)). After you've made changes to a device's user database, you should review the user database to make sure the changes are complete and accurate. For instructions, see [page 2-48](#).

Adding tokens

You can add new tokens that need access to a device. To add tokens, see [page 2-44](#).

Modifying tokens

You can modify a token to change the token's:

- issue code
- time zone number
- expiration date
- deadbolt override setting
- passage mode setting.

Note: Issue codes generally are not used for V Series Keypad Security Devices.

To modify a token:

1. Press ↑ or ↓ until you see:

```
>ADD/MODIFY CARD
DELETE CARD
```

2. Press *. For example, you see:

```
ENTER CARD #
000000
```

3. Type the card number or access code of the token you want to modify, preceded by enough zeros to replace the zeros you see (the total number of digits in the card number or access code for the selected token format). For example, if the card number or access code you want to modify is 57 and the card number or access code for the selected token format has six digits, type **000057**.

4. Press *. For example, you see:

```
ENTER ISSUE CODE
1 (0-9)
```

5. If you want to change the token's issue code, type the new issue code, preceded by enough zeros to replace the zeros you see (the total number of digits in the issue code for the selected token format). For example, if you want the issue code to be 2 and the issue code for the selected token format has one digit, type **2**.

Note: Issue codes generally are not used for V Series Keypad Security Devices.

6. Press *. For example, you see:

```
ENTER TZ #
7 (0-9)
```

7. If you want to change the number of the time zone representing the time periods when you want the token to be able to access the door, type the new time zone number. Type the number of one of the time zones defined for the device (from **1** to **8**), or type **0** for never, or type **9** for always. For information about defining time zones, see [page 2-14](#).

8. Press *. For example, you see:

```
EXPIRE: YY/MM/DD
DATE: 00/12/31
```

9. If you want to change the date when you want the token to expire and no longer be able to access the door, type the new date. Type the year, then the month, then the day. For example, if you want the card to expire on December 31, 2001, type **011231**.

10. Press *. For example, you see:

BOLT OVERRIDE
0=NO 1=YES: 1

11. If you want to change the token's deadbolt override setting, type the new setting. To give the token the deadbolt override privilege, type **1**. If you do not want to give the token the deadbolt override privilege, type **0**. For information about this feature, see [page 2-43](#).

Note: The deadbolt override feature applies only to electronic locks with a mortise deadbolt function chassis.

12. Press *. For example, you see:

PASSAGE MODE
0=NO 1=YES: 0

13. If you want to change the token's passage mode setting, type the new setting. To give the token the passage mode privilege, type **1**. If you do not want to give the token the passage mode privilege, type **0**. For information about this feature, see [page 2-43](#).

14. Press *. You see:

>ADD/MODIFY CARD
DELETE CARD

Deleting tokens



Caution

You can delete any token that no longer needs to access the door controlled by the device.

To maintain the security of your facility, you should delete all inactive tokens.

To delete a token:

1. Press ↑ or ↓ until you see:

>DELETE CARD
ADD CARD RANGE

2. Press *. You see:

ENTER CARD #
000000

3. Type the card number or the access code of the token you want to delete, preceded by enough zeros to replace the zeros you see (the total number of digits in the card number or access code for the selected token format). For example, if the card number or access code of the token you want to delete is 101 and the card number or access code for the selected token format has six digits, type **000101**.
4. Press *. The card is deleted. You see:

>DELETE CARD
ADD CARD RANGE

Adding a range of access cards

You can add a range of consecutively numbered access cards that need access to the door controlled by the device. To add a range of access cards, see [page 2-47](#).

Note: Features involving a range of tokens generally are not used for V Series Keypad Security Devices since the use of consecutive access codes can compromise the security of your access control system.

Deleting a range of access cards

You can delete a range of access cards that no longer need to access the door.

To delete a range of access cards:

1. Press ↑ or ↓ until you see:

>DEL CARD RANGE
CHASSIS TYPE

2. Press *. For example, you see:

STARTING CARD #
000000

3. Type the lowest card number in the range, preceded by enough zeros to replace the zeros you see (the total number of digits in the card number for the selected token format). For example, if the lowest card number is 234 and the card number for the selected token format has six digits, type **000234**.

4. Press *. For example, you see:

ENDING CARD #
000000

5. Type the highest card number in the range, preceded by enough zeros to replace the zeros you see. For example, if the highest card number is 249, type **000249**.

6. Press *. You see:

>DEL CARD RANGE
CHASSIS TYPE

PROGRAMMING A V SERIES SECURITY DEVICE TO OVERRIDE TIME ZONE CONTROL

The four door mode features listed below are similar to the timed access features, but let you override time zone control for a door. When you select a door mode to override time zone control, the selected door mode remains in effect until you restore time zone control for the V Series Security Device.

- **Door lock.** This feature locks down the door, denying all tokens access.
- **Card only.** This feature sets the device to allow access to any token in the device's user database.
- **Facility code only.** This feature sets the device to allow access to any token with a valid facility code.



Caution

If someone loses an access card, the card can be used to access the door during the facility code only time zone. To prevent the access card from being used to access the door, you can disable the facility code only time zone, or you can change the facility code for the door and all of the cards that access it.

- **Door unlock.** This feature sets the door to unlock and remain unlocked.

When you are ready to restore the door to time zone control, you set the device to time zone control again. For example, during an emergency you might use the door lock feature to lock out all employees. When the emergency is over, you restore the device to time zone control.

To lock down a door continuously:

1. Press ↑ or ↓ until you see:

>SET DOOR MODE
CONFIG READER

2. Press *. For example, you see:

>TZ CONTROL
DOOR LOCK

3. Press ↑ or ↓ until you see:

>DOOR LOCK
CARD ONLY

4. Press *. You see:

>SET DOOR MODE
CONFIG READER

To disable time zone control while allowing individual tokens access:

1. Press ↑ or ↓ until you see:

>SET DOOR MODE
CONFIG READER

2. Press *. For example, you see:

>TZ CONTROL
DOOR LOCK

3. Press ↑ or ↓ until you see:

>CARD ONLY
FC-CODE ONLY

4. Press *. You see:

>SET DOOR MODE
CONFIG READER

To allow access for tokens with a valid facility code:

1. Press ↑ or ↓ until you see:

>SET DOOR MODE
CONFIG READER

2. Press *. For example, you see:

>TZ CONTROL
DOOR LOCK

3. Press ↑ or ↓ until you see:

>FC-CODE ONLY
DOOR UNLOCK

4. Press *. You see:

>SET DOOR MODE
CONFIG READER

To unlock the door continuously:

1. Press ↑ or ↓ until you see:

```
>SET DOOR MODE  
CONFIG READER
```

2. Press *. For example, you see:

```
>TZ CONTROL  
DOOR LOCK
```

3. Press ↑ or ↓ until you see:

```
>DOOR UNLOCK  
TZ CONTROL
```

4. Press *. You see:

```
>SET DOOR MODE  
CONFIG READER
```

To restore time zone control:

1. Press ↑ or ↓ until you see:

```
>SET DOOR MODE  
CONFIG READER
```

2. Press *. For example, you see:

```
>DOOR LOCK  
CARD ONLY
```

3. Press ↑ or ↓ until you see:

```
>TZ CONTROL  
DOOR LOCK
```

4. Press *. You see:

```
>SET DOOR MODE  
CONFIG READER
```


VIEWING A V SERIES SECURITY DEVICE'S HISTORY

You can view a V Series Security Device's history, which shows up to the last 1000 events at the device, including the date and time of each event. Each event is an action taken at the door controlled by the device or by the device itself. For example, the device records each programming change made for the device.

The device also records each time it grants access to a token or denies access to a token. For access events, the device records the card number or access code associated with the event.

You might view a device's history to determine why a device is operating differently than you expect. You also might view a device's history if you've had a security problem and want to find out who accessed the door controlled by the device during a certain time period.

To view a device's history:

1. Press ↑ or ↓ until you see:

```
>VIEW DATA BASE  
RESET SYSTEM
```

2. Press *. You see:

```
>VIEW HISTORY  
VIEW CARD DATA
```

3. Press *. You see the most recent (highest-numbered) event recorded in the device's history. For example, you see:

```
ACCESS GRANTED  
1000  
00/08/17 06:25  
CARD # 000411
```

4. To view additional events, press ↑ to view the previous (earlier) event. Press ↓ to view the next (later) event.
5. When you've finished viewing events in the device's history, press # twice. You see:

```
>VIEW DATA BASE  
RESET SYSTEM
```

VIEWING A V SERIES SECURITY DEVICE'S SYSTEM DATA

You can view a V Series Security Device's ROM version number and real time clock number. You might need this information to upgrade a device.

To view a device's system data:

1. Press ↑ or ↓ until you see:

```
>VIEW DATA BASE  
RESET SYSTEM
```

2. Press *. You see:

```
>VIEW HISTORY  
VIEW CARD DATA
```

3. Press ↑ or ↓ until you see:

```
>VIEW SYS DATA  
VIEW HISTORY
```

4. Press *. For example, you see:

```
ROM V02.15  
RTC# 00000000FAFE2
```

5. When you've finished viewing the data, press # twice. You see:

```
>VIEW DATA BASE  
RESET SYSTEM
```

RESETTING A V SERIES SECURITY DEVICE

You can reset a V Series Security Device if you want to restore the factory default settings for the device and reprogram the device. You also can clear the user database without affecting programming settings. For example, you might want to clear the user database if a new group of people need to access the door controlled by the device.



Resetting a device will erase all of the device's programming settings, all of the device's history events, and all of the tokens in the device's user database. Resetting the user database will erase all tokens in the device's user database, but preserve the programming settings and history.

To reset a device's programming settings, history, *and* user database:

1. Press ↑ or ↓ until you see:

```
>RESET SYSTEM
ENTER DATE/TIME
```

2. Press *. You see:

```
>RESET CARD DATA
RESET ALL
```

3. Press ↑ or ↓ until you see:

```
>RESET ALL
RESET CARD DATA
```

4. Press *. You see:

```
>RESET ALL
0=NO 1=YES: 0
```

5. To reset the device, type **1**. If you decide you *do not* want to reset the device, type **0**.

6. Press *. If you typed **1** in Step 5, the device's programming settings, history, and user database are reset to factory default settings. You see:

```
>RESET ALL
RESET CARD DATA
```

7. Press #. You see:

```
>RESET SYSTEM
ENTER DATE/TIME
```

**Caution**

You should add a facility code and a permanent communication token before you close communication with the device. However, if you close communication without adding a new communication token and facility code, the temporary communication token and temporary operator token will work for the device.

To add a facility code, see [page 2-28](#). To add a permanent communication card, see [page 2-42](#).

To reset a device's user database only:

1. Press ↑ or ↓ until you see:

```
>RESET SYSTEM  
ENTER DATE/TIME
```

2. Press *. You see:

```
>RESET CARD DATA  
RESET ALL
```

3. Press *. You see:

```
>RESET CARD DATA  
0=NO 1=YES: 0
```

4. To reset the user database, type **1**. If you decide you *do not* want to reset the user database, type **0**.

5. Press *. If you typed **1** in Step 4, the device's user database is reset to factory default settings. You see:

```
>RESET ALL  
RESET CARD DATA
```

6. Press #. You see:

```
>RESET SYSTEM  
ENTER DATE/TIME
```

CLEARING A LOW BATTERY MESSAGE (ELECTRONIC LOCK ONLY)

If a V Series Electronic Lock has low batteries, the lock rejects all tokens, and the lock's red and green LEDs flash when a user tries to access the lock. The lock also generates a low battery message. Even after the batteries are changed, the lock continues to reject tokens until you clear the lock's low battery message.

To clear an electronic lock's low battery message:

1. When the handheld establishes communication with the electronic lock you see:
2. To clear the low battery message, type **1**.

```
LOW BATT DETECT  
CLEAR LOW BATT? 0
```

3. Press *. You see:

```
>ENTER DATE/TIME  
CONFIG HOLIDAYS
```

A

GLOSSARY

Access card	Credit card-size device encoded with magnetic information and used to access a door controlled by a V Series Magnetic Stripe Security Device or a Proximity Security Device.
Access code	Sequence of digits that is included in a personal identification number (PIN) and identifies the user.
Card Encoder	Device that reads, encodes, and erases information on a V Series access card.
Card Encoding Software	Software that controls the V Series Card Encoder.
Card number	Sequence of digits that is encoded on an access card and identifies the user.
Card only door mode	Door mode that allows access to any token in a V Series Security Device's database.
Chassis type	Type of mechanical locking mechanism—cylindrical or mortise—used in an electronic lock.
Communication token	Token generally used for all V Series Security Devices in a facility to access devices at any time for programming.
Controller	Device that allows the V Series electronics to be separate from a door's locking mechanism and to be located up to 500 feet away from the locking mechanism. The controller provides V Series's electronic features for use with electrically-controlled locking devices.
Cylindrical chassis type	Lock chassis that installs into a circular bore in the door.

Daylight savings time setting	Programming setting that determines whether a V Series Security Device automatically adjusts its clock for daylight savings time.
Deadbolt override privilege	Privilege that can be granted to a token so the token can access a door with a mortise electronic lock even when the door's deadbolt is thrown.
Device	V Series Security Device. Both V Series Electronic Locks and V Series Controllers are V Series Security Devices.
Door forced alarm	Remote alarm triggered by a V Series Controller when the door controlled by the controller is opened without use of a valid access method.
Door lock door mode	Door mode that locks down a door, denying all tokens access.
Door lock time zone	Time zone when a door automatically locks down, denying all tokens access, and then later resumes normal operation.
Door mode	One of five types of operation for a V Series Security Device that determines what access is currently provided at a door.
Door open too long (DOTL) feature	V Series Controller feature that monitors whether the door controlled by the controller has been open too long.
Door unlock door mode	Door mode that sets the door to unlock and remain unlocked.
Door unlock time zone	Time zone when a door automatically unlocks (or unlocks when accessed by a valid token) and then later relocks.
Electronic lock	Battery-powered, self-contained, programmable V Series lock, which controls access to a door. V Series Electronic Locks include magnetic stripe electronic locks, proximity electronic locks, and keypad electronic locks.
Enrolling station	Device that can be connected to a PC running the IPS and used to read proximity cards while adding token records to a device configuration used by proximity security devices.
Facility code	Sequence of digits that generally is unique and programmed into every device and encoded on every access card, or included in every personal identification number (PIN), belonging to a facility to help ensure the security of a facility's doors.
Facility code only door mode	Door mode that sets a device to allow access to any token with a valid facility code.
Facility code only time zone	Time zone when all tokens with a valid facility code can access a door.
Handheld terminal	Equipment that lets you program a V Series Security Device with parameters and view access control information, such as the user database, programming settings, and event history.
History	Chronological record of up to the last 1000 events at a V Series Security Device, including the date and time of each event.
Holiday	Time period of any length defined for a V Series Security Device, and usually associated with a calendar holiday.

Intelligent Programmer Software (IPS)	Software that lets you define programming settings and the user database for groups of V Series Security Devices, as well as individual devices. The IPS also lets you retrieve the history records from devices, as well as view and print device information.
Intelligent Programmer Software (IPS) for Windows	Windows-compatible software that lets you define programming settings and the user database for groups of V Series Security Devices, as well as individual devices. The IPS for Windows also lets you retrieve the history records from devices, as well as view and print device information.
Issue code	Number indicating how many times a particular card number or access code has been issued.
Look ahead setting	Feature that lets you program a V Series Security Device to accept a token whose encoded issue code is higher than the current issue code recorded in the device's database.
Mortise chassis type	Lock chassis that installs into a mortised cavity in the edge of a door.
Passage mode privilege	Privilege that can be granted to a token for a door. When the token is used a twice (within the unlock duration) during the time zone assigned to the token, the door remains unlocked. When the door is unlocked by passage mode, and the token is used twice (within the unlock duration), the door relocks.
Password	One to six digits used with a communication token to access a V Series Security Device for programming.
Personal identification number (PIN)	Sequence of digits, which generally includes a facility code and an access code that identifies the user. A user enters a PIN to access a door controlled by a V Series Keypad Security Device.
Reader	Device that can be connected to a V Series Controller. Users use their tokens at the reader to access the door protected by the controller.
Remote unlock device	Device, such as a button, that can be connected to a V Series Controller and located away from the door. When someone, such as a receptionist, presses the remote unlock button, the controller unlocks the door if the controller is programmed for the remote unlock feature.
Request-to-exit device	Device, such as a button, that can be connected to a V Series Controller. When someone activates the request-to-exit device, the controller does not trigger an alarm. If the controller is programmed for the RQE unlock feature, the controller also unlocks the door.
Temporary communication token	Token for temporary use that lets you communicate with a V Series Security Device programmed with factory default settings.
Temporary operator token	Token that gives people temporary access to doors before the devices in a V Series System are permanently programmed.
Time interval	Block of time during a time zone.
Time zone	Blocks of time (up to three time intervals) that occur weekly and/or on holidays, and determine when selected tokens can access a door or when a special access feature is in effect.

Time zone control door mode	Door mode that lets timed access features determine the operation of a V Series Security Device.
Token	Access card or personal identification number (PIN) used to access a door.
Unlock duration	Number of seconds that a door remains unlocked when accessed by a valid access method.
User database	All tokens—up to 1000—defined for a V Series Security Device.
Validate LRC setting	Feature that determines whether a V Series Security Device validates the longitudinal redundancy check (LRC) for a token. The LRC, included in most token formats, helps verify that the token data is interpreted correctly.
Variable card format	Feature that lets you program a V Series Security Device to accept tokens with a particular format.